Together we learn, together we succeed

Online Safety Policy 2023

Approved by:	Rusper Full Governing Board	**Date:**	17.10.23
Last reviewed on:			
Next review due by:	October 2024		

Purpose

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

As a school, it is essential that children are safeguarded from potentially harmful and inappropriate online material. Rusper Primary School's approach to Online Safety is to protect and educate pupils and staff in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Rusper Primary School's activities.

Scope

This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance.

Legal Framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- Keeping Children Safe in Education
- Online Abuse
- Bullying
- Child Protection.

Policy development

This policy has been developed in consultation with staff, pupils and parents. The consultation and policy development process involved the following steps:

1. Review – the Online Safety leader gathered all relevant information including relevant national and local guidance
2. Contextual data – the Online Safety leader gathered contextual data relating to pupil demographics and historical data at Rusper Primary School
3. Staff consultation – all school staff were given the opportunity to look at the policy and make recommendations
4. Parent/carer consultation – parents and carers are invited to raise questions about the policy
5. Ratification – once amendments were made, the policy was shared with governors and ratified

Roles and responsibilities

The governing board

The governing board will approve the Online Safety policy, and hold the designated leaders to account for its implementation.

The Head Teacher / Designated Safeguarding Lead

The Headteacher / Designated Safeguarding Lead has ultimate responsibility for ensuring that Online Safety is established and rigorously maintained for all pupils at Rusper Primary.

The Designated Safeguarding lead at Rusper Primary is **Nick Avey**

Designated Leader for Monitoring and Filtering Systems

The designated leader for Monitoring and Filtering Systems will work closely with the IT service provider to ensure effective monitoring and filtering.

The designated Monitoring and Filtering lead at Rusper Primary is **Michael Snook**

Subject leader

The Computing and RSHE subject leaders are responsible for ensuring that Online Safety is taught consistently across the school.

Staff

Staff are responsible for:

- Delivering teaching of Online Safety in accordance with this policy
- Modelling positive attitudes to Online Safety
- Monitoring knowledge
- Responding to the needs of individual pupils

Pupils

Pupils are expected to engage fully in Online Safety, being respectful and sensitive to different cultural traditions and Online Safety

Online Safety Issue Classification:

At Rusper, we understand that the breadth of issues classified within online safety in considerable and ever evolving, but can be categorised into four areas of risk (The 4 C's)

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

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

By using the four areas of risk (Content, Contact, Conduct and Commerce), leaders, staff and governors at Rusper Primary School are better able to understand the extent and breadth of online safety concerns and adapt/apply support accordingly.

We Believe That:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We Recognise That:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether or not they are using Rusper Primary School's network and devices
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- Appointing an online safety coordinator – **Michael Snook**
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- Supporting and encouraging the young people in our school to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Supporting and encouraging parents and carers to do what they can to keep their children safe online
- Developing an online safety agreement for use with young people and their parents or carers
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- Reviewing and updating the security of our information systems regularly
- Ensuring that user names, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- Providing supervision, support and training for staff and volunteers about online safety
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

In the first instance, Rusper Primary School will foster positive attitudes to online safety and directly teach safe online behaviours for all our pupils. Both our Computing and our Relationship, Sex and Health Education (RSHE) curriculums contain specific sections on Online Safety (see Curriculum section below for more detail).

Where a pupil demonstrates an unsafe behaviour online, the school response will be determined by the extent of concern.

Low-level behaviour concerns (e.g. deviating from teacher instruction e.g. searching for information not related to the designated topic in class) will be dealt with in line with following low-level procedures within our Behaviour Policy (E.g. loss of privilege combined with teacher led reflection and speaking with parents if the behaviour persists)

Where a pupil demonstrates a more serious unsafe online behaviour online themselves ie abuse of others (eg online bullying or perpetrating harmful sexual behaviours), the behaviours will be treated as a serious safeguarding concern. Such behaviours will be dealt with in line with school safeguarding procedures and with serious negative behaviour procedures within our Behaviour Policy. For safeguarding procedures see below. For behaviour procedures, depended on the severity and extent of the behaviour, sanctions will range from fixed-term internal exclusion to fixed-term external exclusion or even permanent external exclusion. The extent of sanction will be applied on a case-by-case basis at the discretion of the Headteacher. All sanctions will be combined with tailored support programs for the child and their family, aimed at reducing the chance of repeated behaviours in the future.

Where the school becomes aware that the child may be the victim of online abuse eg grooming or harmful sexual behaviour, the school responses will follow safeguarding procedures.

In all instances of safeguarding concerns, the child's parents will be informed directly. Subsequently, the school designated safeguarding team will accurately identify the category of online abuse (specified above with the 4 C's) and then apply a risk threshold assessment using the West Sussex Continuum of Needs Threshold tool.

- Level 1: Where the risk level suggests the child and family can be supported effectively through in school provision, depended on the behaviour, a combination of sanctions will be applied with the agreement of parents and child and a tailored provision program will be applied.
- Level 2: Where the risk level suggests the child and family may need the support of an external service alongside school support, parental consent will be sought and a referral will be made to the integrated front door (Multi-agency service hub). The case will then be considered externally and decision-making about the next steps will be applied via the Local Authority Early Help Team.
- Level 3: Where the risk level suggests the child and family have a more urgent or complex need, and/or where there is a greater degree of vulnerability to the child, parental consent will be sought and a referral will be made to the integrated front door (multi-agency service hub). The case will then be considered externally and decision-making about the next steps will be applied via the Local Authority Early Help Team and a Team around the Child (TAC), or a targeted coordinated response from the Multi Agency Team will be required.
- Level 4: Where the risk level suggest that the needs of the child have been significantly compromised and/or they are suffering significant harm or impairment, then a statutory and/or specialist intervention will be required to keep the child safe. Here, a comprehensive statutory assessment under Section 17 of the Children Act 1989 will be required. Intervention under Section 47 of the Children Act 1989 may also be required for those children who are at immediate risk of significant harm. Legal action may need to be taken and the Local Authority may need to accommodate the child in order to ensure their protection.

In order to ensure that any problems have been resolved in the long term, there will be regular opportunities to review any interventions / support plans developed to address online abuse

There will also be annual reviews of all safeguarding related policies and procedures to ensure that they are current, up to date and working correctly.

This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- photography and image sharing guidance.

Monitoring and Filtering

As it is Rusper Primary School's responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, leaders, staff and governors are driven to limit (as reasonably as they can) children's exposure to risks from the school's IT system. As part of this, Rusper Primary school has put in place an appropriate filtering and monitoring system and will regularly review its effectiveness. It is vital that leaders and relevant staff have an awareness and understanding of provisions in place and manage these effectively, but also to ensure that staff know how to escalate concerns when identified. To support this duty, Rusper Primary School works alongside the 'Filtering and Monitoring Standards' set out by the Department for Education. These standards set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs.

The designated member of the Designated Safeguarding Team responsible for Monitoring and Filtering at Rusper Primary School is **Michael Snook**

The DSL responsible for Monitoring and Filtering will complete and conduct a Monitoring and Filtering action plan. The plan will include

- Scheduled monitoring of pupil online activity in school
- Scheduled review of the school filtering systems in liaison with the school's technical support team at JSPC
- Consult with the DSL team to agree decisions in response to concerns
- Complete actions in response to concerns
- Complete records of any actions taken in response to concerns
- Document decisions taken on what is blocked and why
- Provide reports

Curriculum

At Rusper Primary School, we set an ethos that Online Safety is part of our Safeguarding Curriculum. It does mean that Online Safety is taught in Computing and Relationships, Social and Health Educations (RSHE) but it also allows us to embed good Online Safety practice throughout the academic year. Other examples of when Online Safety might be taught are:

- Using computers to research a particular subject in lessons such as History and Science
- Safer Internet Day
- Anti-Bullying Week
- Appropriate use on online work supporting Home Learning

Our Computing Curriculum and RSHE curriculum offer the most opportunities to deliver Online Safety teaching. See below for key details on those curriculum areas and how Online Safety is taught.

Kapow

Kapow Primary offers full coverages of the Key Stage 1 and Key Stage 2 Computing curriculum where every year group has a dedicated online safety unit to address the risks and challenges faced by primary school pupils growing up in an ever increasingly online world. The Kapow Computing has 4 overarching themes that focus the teaching of online safety. Below, you can find a table showing these 4 themes plus extra information on what is covered across the curriculum in these areas:

Underpinning knowledge and behaviours	**Harms and risks**	**How to stay safe online**	**Wellbeing**
➢ How to evaluate what they see online ➢ How to recognise techniques used for persuasion ➢ Online behaviour ➢ How to identify online risks ➢ How and when to seek support ➢ Online media literacy strategy	➢ Age restrictions ➢ How content can be used and shared ➢ Disinformation, misinformation, malinformation and hoaxes ➢ Fake websites and scam emails ➢ Fraud (online) ➢ Password phishing ➢ Personal data ➢ Persuasive design ➢ Privacy settings ➢ Targeting of online content	➢ Abuse (online) ➢ Challenges ➢ Fake profiles ➢ Live streaming ➢ Unsafe communication	➢ Impact on confidence (including body confidence) ➢ Impact on quality of life, physical and mental health and relationships ➢ Online versus offline behaviours ➢ Reputational damage

RSHE

As part of our RSHE curriculum, designed in collaboration with West Sussex County Council, children are given opportunities to focus their learning on online safety with specific topics aimed at teaching them the skills and knowledge needed. Below is a table showing the Online Safety topics and when they are taught as part of the RSHE curriculum:

	Year 1 and 2 Cycle 1	**Year 1 and 2 Cycle 2**	**Year 3 and 4 Cycle 1**	**Year 3 and 4 Cycle 2**	**Year 5 and 6 Cycle 1**	**Year 5 and 6 Cycle 2**
A1						

A2						Appropriate age online and access to information
Sp 1		Digital footprints and using tech	Where information comes from and reliable sources			Identities online and influence
Sp 2	Online activities and sources of internet information	Communicating online (being safe and cyberbullying)	Online profiles and fake news		Online friendships, staying safe online and decision making/ influences	
Sum1			Bullying (inc cyber) Pressure to share and dares – including cyber			
Sum 2						

Awareness and Engagement with Parents/Carers

Rusper Primary School recognises that parents and carers have an essential role to play in enabling our pupils to become safe and responsible users of the internet and associated technologies.

We will ensure parents and carers understand and are aware of:

- the systems used at school to filter and monitor their child's online use by providing information in our home-school agreement and Acceptable Use Policy.
- what their children are being asked to do online, including the sites they will asked to access by providing information in our home-school agreement and Acceptable Use Policy.

We will build a partnership approach and reinforce the important of online safety through regular contact and communication with parents and carers by:

- providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training
- drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus and on our website.
- requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
- requiring them to read our acceptable use of technology policies and discuss the implications with their children.

Safer Use of Technology

Classroom Use

Rusper Primary School uses a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet, which may include search engines and educational websites
- Digital cameras, webcams and video cameras.

All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The school will use appropriate search tools Squiggle for pupils) as identified following an informed risk assessment.

Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. This includes using supervised educational versions of video sharing platforms with children or for adult educational use. Any videos viewed should be previewed before sharing as a teaching tool with children.

We will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information. Supervision of internet access and technology use will be appropriate to pupils age and ability. This includes:

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.

Key Stage 2

- Pupils will use age-appropriate search engines and online tools.
- Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils age and ability.

Managing internet access

All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, before being given access to our computer system, IT resources or the internet. We will maintain a record of users who are granted access to our devices and systems.

Social Media

Expectations

- Rusper Primary School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.
- All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control pupils and staff access to social media whilst using school provided devices and systems on site.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL and/or Head of School prior to use. Any use will take place in accordance with out our remote learning Acceptable Use Policy.

- Concerns regarding the online conduct of any member of Rusper Primary School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff code of conduct, Acceptable Use Policies, and Child Protection.

Staff use of social media

- The use of social media during school hours for personal use is not permitted for staff.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct policy and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and safeguarding policies.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.
- Members of staff are encouraged not to identify themselves as employees of Rusper Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Official use of social media

- Rusper Primary School official social media channels are:
    - Twitter link;
- The official use of social media sites by Rusper Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the Head Teacher prior to use.
- Official social media sites are suitably protected and, where possible, run and linked to our website.

    - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents and carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with pupils; any official social media activity involving pupils will be moderated if possible and written parental consent will be obtained as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read and understand our Acceptable Use Policy.
    - Be aware they are an ambassador for the school.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any private or direct messaging with current or past pupils or their family members.
    - Inform the DSL (or deputies) and/or the Head Teacher of any concerns, such as criticism, inappropriate content or contact from pupils.

Pupils use of social media

- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents and carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another pupils, could have repercussions for the orderly running of the school when the pupils is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.
- Rusper Primary will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and

respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies.

- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher.
- Pupils will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords. o to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the setting and externally.
- Any concerns regarding pupils use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputies) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding pupils use of social media will be shared with parents and carers as appropriate, particularly when concerning underage use of social media services and games.

Mobile and Smart Technology

Safe use of mobile and smart technology expectations

Rusper Primary School recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents and carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Rusper Primary School community are advised to:
    - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used by children in any area on the school site. If a child does bring a phone into school (e.g. for communication with parents/carers as they travel home on the bus), the device must be left with the office staff.
- Staff may use their mobile phone in the staffroom or a room where no child is present.
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of the Rusper Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

Staff use of mobile and smart technology

Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security, staff behaviour/code of conduct and Acceptable Use Policies.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (list details, for example, locked in a locker/drawer) during lesson time.
- Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- Not use personal devices during teaching periods unless verbal permission has been given by the Head Teacher, such as in emergency circumstances.
- Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers without prior arrangement with the Head of School.

- Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the Head Teacher.

Staff will only use school provided equipment (not personal devices):

- to take photos or videos of pupils in line with our image use policy.
- to work directly with pupils during lessons/educational activities.
- to communicate with parents and carers.

Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Head Teacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

If a member of staff breaches our policy, action will be taken in line with our staff code of conduct and policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Visitors' use of mobile and smart technology

Parents and carers and visitors, including volunteers and contractors, are expected to ensure that:

- they do not use a mobile phone in the school
- where appropriate the senior leadership may give permission to take a photo of their own child eg: Christmas Nativity Play
- Appropriate signage and visitors' information leaflets are in place to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.

- If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the Head Teacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or Head Teacher of any breaches of our policy.