Rusthall St Paul's CE School
Online Safety Policy

(based on KCC exemplar policy)

Key Details

Designated Safeguarding Lead (s): (Caroline Powell, Headteacher)

Named Governor with lead responsibility: (Deborah Bruce)

Date written: November, 2017

Latest review: April 2020

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

Page no

Rusthall St Paul's CE PrimarySchool Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Rusthall St Paul's involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" September 2019, Early Years and Foundation Stage2017 and the Kent Safeguarding Children Board procedures.

- The purpose of Rusthall St Paul's online safety policy is to:
  - Safeguard and protect all members of Rusthall St Paul's community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- Rusthall St Paul's identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- Rusthall St Paul's believes that online safety is an essential part of safeguarding and acknowledges it'sduty to ensure that all pupils and staff are protected from potential harm online.
- Rusthall St Paul's identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Rusthall St Paul's believes that pupilsshould be empowered to build resilience andtodevelop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Anti-bullying policy
  - Acceptable Use Policies (AUP) and/or the Code of conduct

  - Behaviour and discipline policy
  - Child protection policy
  - Confidentiality policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
  - Data security
  - Cameras and image use policy
  - Searching, screening and confiscation policy

3. Monitoring and Review

- Rusthall St Paul's will review this policy at least annually
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- The school will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report at least annually to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The school has appointed Caroline Powell, as Designated Safeguarding Lead to be the online safety lead.
- Rusthall St Paul's recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of Rusthall St Paul's life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoringsystems are in place.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

- Ensure there are robust reporting channels in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, pupils and parents/carers are proactively engaged in activities whish promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues
- Liaise with other members of staff such as IT technicians and the SENCo on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSL to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community,as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, and school policies and procedures.
- Report online safety concerns, as appropriate,to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility forsafeguarding and online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Readand adhere to the online safety policy and acceptable use of technology polices.
- Take responsibility for the security of IT systems and the electronic data they use, or have access to.

- Model good practice when using technology with pupils.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identifyonline safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signpostingchildren and parents / carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures*(including password policies and encryption)*as directed by the leadership team to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems if given to the DSL or deputy to enable them to take appropriate safeguarding action when required

4.5 It is the responsibility of pupils(at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriateonline safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the schoolacceptable use of technology and behaviour policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if theyare concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their childrenand reinforcing appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement.
- Abide by the school's home-school agreement and/or AUPs.Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.

- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Educationand engagement with pupils

- The school will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring our curriculum and whole school approach is developed in line with ‘Teaching online safety in school’.
    - Ensuring online safety is addressed in PSHE, SRE and Computing programmes of study, covering use both at home school and home.
    - Reinforcing online safety messages in other curriculum subjects as appropriate and whenever technology or the internet is in use.
    - Implementing appropriate peer education approaches.
    - Creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and /or being judged for talking about something which happened to them online.
    - Involving the DSL or deputy as part of planning or online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content.
    - Making informed decisions to ensure that any educational resources used are appropriate for our pupils.
    - Using external visitors, where appropriate, to complement and support our internal online safety education approaches.
    - Providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
    - Rewarding positive use of technology.

- Rusthall St Paul’s will support pupils to understandand follow our AUP in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing pupilsthat network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.

- Rusthall St Paul’s will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - Ensuring age appropriate education regarding safe and responsible use precedes internet access.
    - Teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
    - Educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
    - Enabling them to understand what acceptable and unacceptable online behaviour looks like.

- Preparing them to identify possible online risks and make informed decisions about how to act and respond.
- Ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.1.1 Vulnerable Pupils

- Rusthall St Paul's recognises that any pupil can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some pupils, for example looked after children, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss , who may be more susceptible or may have less support in staying safe online .
- Rusthall St Paul's will ensure that differentiated and ability appropriate online safety education,access and support is provided to vulnerable pupils.
- Rusthall St Paul's will seek input from specialist staff as appropriate, including theDSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's need.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staffwhich is integrated, aligned and considered as part of our overarching safeguarding approach. This will be though our annual safeguarding update training, specific online safety sessions and bulletins / updates to staff.
- Staff training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.
- Build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media,could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

- Rusthall St Paul's recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

- The school will build a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats. This may include offering specific online safety awareness training and highlighting online safety at otherevents which could include parent evenings.
  - Drawing their attention to the school online safety policy and expectations in newsletters, letters, in our prospectus and on our website.
  - Requesting that they read online safety information as partof joining our school, for example, within our home school agreement.
  - Requiringthemto read the school AUP and discuss its implications with their children.

6. Reducing Online Risks

- Rusthall St Paul's recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannotbe accessed via a school computer or devices and as such identify clear procedures to follow is breaches or concerns arise.
- All members of the school community are made awareof the school's expectations regarding safe and appropriate behaviour onlineand the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Rusthall St Paul's uses a wide range of technology. This includes access to:
  - Computers, tablets and other digital devices
  - Internet which may include search engines and educational websites
  - Email
  - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school'sAUP and with appropriate safety and security measures in place. At Rusthall we have a general AUP and an AUP for mobile devices.
- 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 age appropriate search tools e.g. Google Safe Search, Dorling Kindersley find out, CBBC safe search following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school 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 pupils will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Pupils' 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.
        - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- The school will maintain arecord of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign anAUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Rusthall St Paul's governors and leadershave ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leadersare aware of the need to prevent"over blocking",as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through EIS.
- The school uses Lightspeed which blocks access to sites which could promote or include harmful and / or inappropriate behaviour or material. This includes content which promotes discrimination or extremis, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self – harm, eating disorder and /or suicide content, pornographic content and violent material.
- The school is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
- The school integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

Dealing with Filtering breaches

- We work with EIS to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
    - If pupils discover unsuitable sites, they will be required to report it immediately, to turn off the monitor and report the concern to the member of staff teaching them.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.3 Appropriate Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring (supervision), monitoring internet and web access (reviewing logfile information)

- The school has a clear procedure for responding to concerns identified via monitoring approaches. The DSL will respond in line with the child-protection guidance and if necessary will seek further advice from the KCC safeguarding officer or e-safety officer.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in the schools information security policy which can be accessed at www.rusthall-cep.kent.sch.uk

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on the school’s network, as required and when deemed necessary by leadership staff.

    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
    - The appropriate use of user logins and passwords to access the school network.
        - Specific user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- In Reception pupils log in under adult supervision. From Year 1 all pupils log in to the system under adult supervision. For Purple Mash they have their own username and password. For KS2 pupils have their own username.
- We requireall adult users to:
    - Use strong passwords for access into our system.
    - Change their passwords everythree months.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.
    - Lock access to devices/systems when not in use.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on ourwebsite meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that ourwebsite complies with guidelines for publications including: accessibility; data protection;respect for intellectual property rights; privacy policies and copyright.
- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, and safeguarding policy.

7.8 Managing Email

- Access to school email systems will always take place in accordance withData protection legislation and in line with other school policies,including:Confidentiality, AUPs and Code of conduct.

    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which containssensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell Caroline Powell (DSL) or deputy if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school. Staff may only check their personal accounts during their undirected time.

7.8.1 Staff Email

- All members of staff are provided with a specific school email address, to use for all official communication: the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents. Staff will respond to emails within three working days and are not expected to respond immediately.

7.8.2 Pupils Emails

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school

7.9Educational use of Videoconferencing and/or Webcams

- Rusthall St Paul's recognise that videoconferencinganduse of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencingandwebcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publically.
    - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability. A member of staff will be present to oversee.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site,staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Learning Platforms

Rusthall St Paul's does not currently use a learning platform.

7.11 Management of Applications (apps) used to Record Children's Progress

- The school uses Class Dojo and Tapestry to track pupils progress and/or share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such,she will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection Legislation.
- In order to safeguard pupils data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
    - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access;for example,not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Rusthall St Paul's community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Rusthall St Paul's community areexpected to engage in social media in a positive, safe and responsible manner, at all times.
  - All members of Rusthall St Paul's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site. Access to social media during lesson time e.g. blogging is done under the supervision of the class teacher. The school Facebook page is monitored by the Deputy head who is also responsible for posting information
  - The use of social media during school hours for personal use, staff only, is only permitted during non-directed time and not on school technology.
  - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Rusthall St Paul's community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protectionpolicies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction (Code of Conduct) and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within theAUP.

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they 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 sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites as strictly as they can.

  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Using strong passwords and keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Rusthall St Paul's on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.
  - 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 in the school.

8.2.2 Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with the headteacher.
  - Decisions made and advice provided in these situations will be formally recorded in order to safeguard pupils, the setting and members of staff.
  - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts for children.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:

    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications and report concerns both within school and externally.

8.4 Official Use of Social Media

- Rusthall St Paul's official social media channel is: Facebook
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
    - Senior Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official school social media channels.
    - Official social media sites are suitably protected and, where possible, run and are linked to our school website.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including:Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, 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.
    - Only social media toolswhich have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving pupils will be moderated by the school where possible.
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- The school 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.

8.4.1 Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, theywill:
    - Sign the school'sSocial media acceptable use policy.
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times 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 andEqualities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- Rusthall St Paul's recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies,including, but not limited to: Anti-bullying, Behaviour and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of Rusthall St Paul's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of Rusthall St Paul's community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing areas and toilets.

- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of ourBehaviour and Anti-bullying policies.
- All members of Rusthall St Paul's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the schoolBehaviour or Child protection policies.
- Personal mobile devices connected to the school wi-fi should only be used for educational purposes.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law,as well as, relevant school policy and procedures,such as:Confidentiality, Child protection, Data security and Acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time e.g. locked in drawer or handbag/briefcase.
    - Keep mobile phones and personal devices switched off or switched 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 usepersonal devices during teaching periods, unless priorpermission has been given by the headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could underminethis, will be discussed with the Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose (unless they have prior permission from the Headteacher).
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations 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, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.3 Pupils’ Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Rusthall St Paul's expects pupil’s personal devices and mobile phones to be given into the school office at the beginning of the day where they will be locked in a drawer until home time.

- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone in the office.
    - Parents are advised to contact their child via the school office during school hours.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from the Head Teacher.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Head Teacher.
- Mobile phones and personal devices must not be taken into tests.
    - Pupils found in possession of a mobile phone or personal device during a test will be reported to the appropriate body. This may result in the withdrawal from that test.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
    - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Child Protection, Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
    - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf
    - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors, including volunteers and contractors should ensure that mobile phones and devices are not used in public areas where the children are and are only permitted in the staffroom or offices.
- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first,to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about Pupils Online Behaviour and/or Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection risks in line with our Child Protection Policy.
    - The DSL will record these issues in line with the school's child protection policy.
- Rusthall St Paul's recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers: all online peer on peer abuse concerns will be responded to in line with our child protections and behaviour policies.
- The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and / or pastrol support will be offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- The school will inform parents and carers of any online incidents or concerns involving their child, as and when required.

10.2 Concerns about Staff Online Behaviour and / or Welfare

- Any complaintabout staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and / or legal action will be taken in accordance with the Behaviour policy and Code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer Online Behaviour and/or Welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the DSL. The DSL will respond to concerns in line with existing policies, including but not limited to Child Protection, Anti-Bullying, Complaints, Allegations Against Staff, AUP and Behaviour Policies.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11.Procedures for Responding to Specific OnlineIncidents or Concerns

11.1 Online sexual violence and sexual harassment between children

- Our DSL and appropriate members of staff have accessed and understood the DfE 'sexual violence and sexual harassment between children in schools and colleges' (2018) guidance and part 5 of 'Keeping children safe in education'2019.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our Child Protection Policy.
- Rusthall St Paul's recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - Non-consensual sharing of sexual images and videos
    - Sexualised online bullying
    - Online coercion and threats
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence.
    - Unwanted sexual comments and messages on social medial
    - Online sexual exploitation.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

    - If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching and screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
    - If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the policy first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Rusthall St Paul's recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Rusthall St Paul's recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Rusthall St Paul's will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a rangeofage and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between pupils.

11.2Youth Produced Sexual Imagery or "Sexting"

- Rusthall St Paul's recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue;therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCBguidance: "Responding to youth produced sexual imagery".
    - Youth produced sexual imagery or 'sexting' is defined as the production and /or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purpose of indecent images, as anyone under the age of 18.
- Rusthall St Paul's will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing your produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods e.g. visitors to school, as part of lessons/PSHE (where appropriate)
- The school will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.

- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.

        If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - Send, share, save or make copies of content suspected to be in indecent image/video of a child (ie youth produced sexual imagery) and will not allow or request pupils to do so.
- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
    - Act in accordance with ourChild protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Ensure the Designated Safeguarding Lead responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely.
        - If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching, screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
    - Carry out a risk assessment in line with the UKCIS and KSCMP guidance which considers the age andvulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate,about the incident and how it is being managed and provide support and signposting, as appropriate.
    - Make a referral to Children's Services Social Work Service and/or the Police, as appropriate in line with the UKCIS and KSCMP guidance.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCISguidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3Online Child Sexual Abuse and Exploitation

- Rusthall St Paul's recognises online abuse and exploitation,including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead in line with our Child Protection Policy.

- Rusthall St Paul's will ensure that all members of the community are aware of online child abuse, and sexual or criminal exploitation, including:the possible grooming approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is used to report online child sexual abuse is available to pupils and other members of the school community.
- If the school are made aware of incident involving online sexual abuse of a child, the school will:
    - Act in accordance with the school's Child protection and Safeguarding policies and the relevant KSCMP procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices containing evidence securely.
        - If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - If appropriate, make a referral to Children's Social Work Service and inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - Provide the necessary safeguards and support for pupils, such as,offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on/off school premises, using school or personal equipment.
    - Where possible and appropriate pupils will be involved in decision making and if appropriate, will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed,the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the Designated Safeguarding Lead.
- If members of the public or pupils at other schools are believed to have been targeted, the DSL will seek support from Kent Police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4Indecent Images of Children (IIOC)

- Rusthall St Paul's will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.

- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOCby using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
  - Act in accordance with the schools child protection and safeguarding policy and the relevant KSCMP procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the headteacher is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Quarantine any devices until police advice has been sought.

11.5Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Rusthall St Paul's.
- Full details of how the school will respond to cyberbullying are set out in theAnti-bullying policy.

11.6Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Rusthall St Paul's and will be responded to in line with existing school policies, including Child Protection,Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, orwhether a criminal offence has been committed,the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Service and/or Kent Police.

11.7 Online Radicalisation and Extremism

- As listed in this policy, the school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- Ifthe school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child ProtectionPolicy.
- Ifthe school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child Protection and Allegations Policies.

Responding to an Online Safety Concern

Key Local Contacts

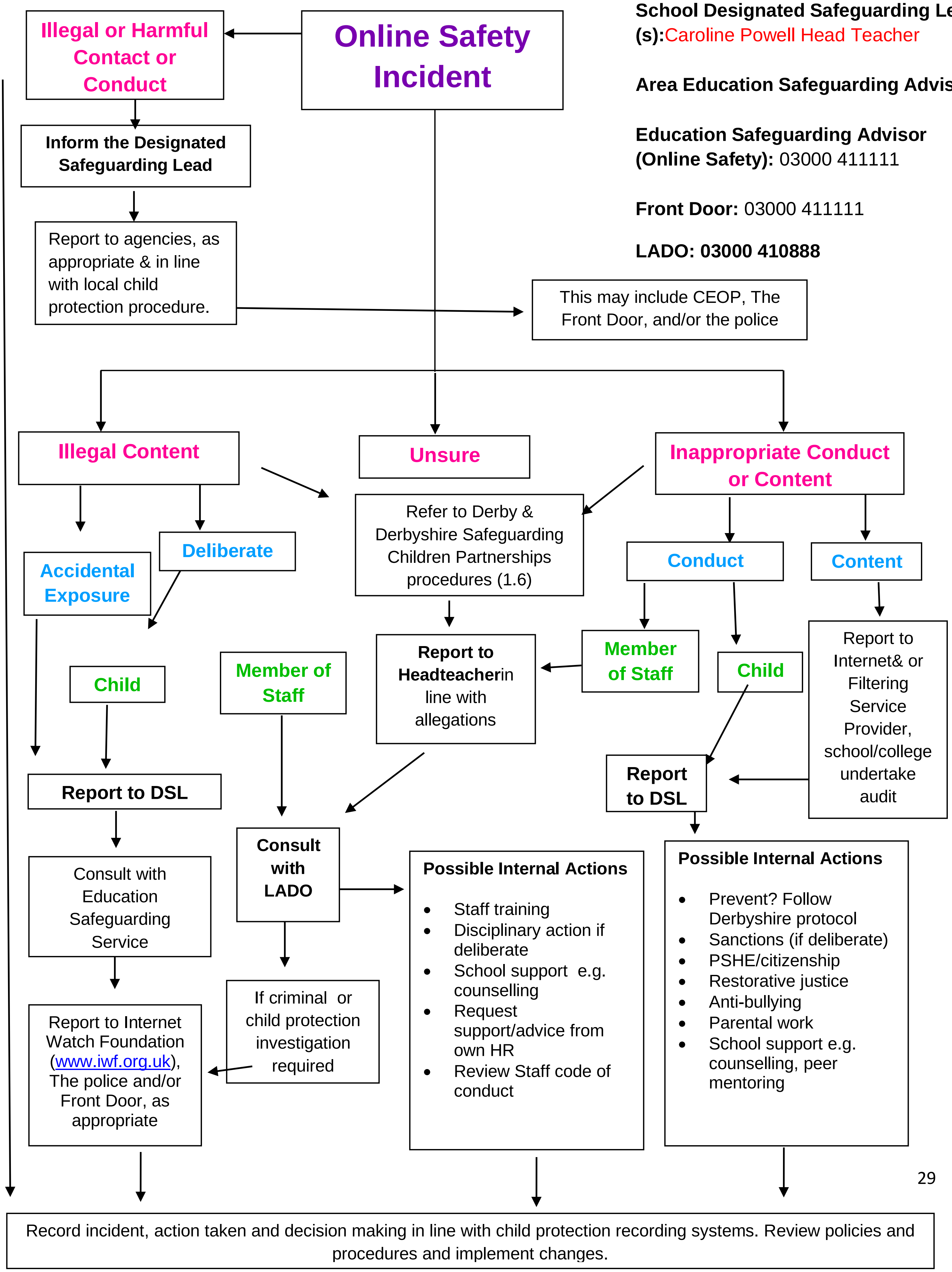
School Designated Safeguarding Lead (s): Caroline Powell Head Teacher

Area Education Safeguarding Advisor:

Education Safeguarding Advisor (Online Safety): 03000 411111

Front Door: 03000 411111

LADO: 03000 410888



Online Safety Incident

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate & in line with local child protection procedure.

This may include CEOP, The Front Door, and/or the police

Illegal Content

Unsure

Inappropriate Conduct or Content

Refer to Derby & Derbyshire Safeguarding Children Partnerships procedures (1.6)

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Report to Internet Watch Foundation (www.iwf.org.uk), The police and/or Front Door, as appropriate

Consult with LADO

If criminal or child protection investigation required

Report to Headteacherin line with allegations

Conduct

Content

Member of Staff

Child

Report to DSL

Report to Internet& or Filtering Service Provider, school/college undertake audit

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate
- School support e.g. counselling
- Request support/advice from own HR
- Review Staff code of conduct

Possible Internal Actions

- Prevent? Follow Derbyshire protocol
- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring

Record incident, action taken and decision making in line with child protection recording systems. Review policies and procedures and implement changes.

12. Useful Links for Educational Settings

Kent Support and Guidance

Education Safeguarding Service, The Education People:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
  - esafetyofficer@kent.gov.uk Tel: 03000 415797
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- Inan emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5 pm / Urgent calls only) please contact 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:**www.eiskent.co.uk

National Links and Resources for settings, pupils and parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk

Staff Acceptable Use Policy APPENDIX 1

As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password; a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly. See on-line safety policy.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998.
   - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
   - Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
   - Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment or via VPN.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces. Policy attached.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead (Caroline Powell) as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT lead (Sandra Sheldrake) as soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries, and will be transparent and open to scrutiny at all times.
    - All communication will take place via school approved communication channels such as a school provided email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead or headteacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Online Safety policyand will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school Code of Conduct and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Caroline Powell).

18. I will agree to abide by the rules in the school acceptable use policy for i-pads.

19. I understand that my use of the school information systems, including any devices provided by the school, school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

20. I understand that the school may exercise its right to monitor the use of ~~i~~nformation systems, including internet access and the interception of emails, in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Rusthall St Paul's Staff Acceptable Use Policy

Name …………………………… Signed …………………………… Date ……………………………

Accepted by …………………………… Date …………………

APPENDIX 2

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school community and allows access for education use. Staff may be given the Wi-Fi code to allow personal equipment to access the Wi-Fi. However when using personal equipment such as phones in school guidelines from the On-line safety policy should be followed at all times. The password should not be given to anyone else unless authorisation has been granted from the DSLs.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

3. The use of ICT devices falls under Rusthall St Paul's school's Acceptable Use Policy, online safety policy and behaviour policy and safeguarding policy. which all students/staff/visitors and volunteers must agree to, and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

8. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other

internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.

12. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal orinappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Leads (Caroline Powell) as soon as possible.

15. If I have any queries or questions regarding safe behaviour online then I will discuss them with Designated Safeguarding Leads (Caroline Powell).

16. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Rusthall St Paul's school Wi-Fi Acceptable Use Policy.

Signed: ……………………….... Print Name: ……………………… Date: ………

Accepted by: ………………………….. Print Name: ………………………….

APPENDIX 3

Staff Social Networking Acceptable Use Policy

For use with staff running official school social media accounts

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that Facebook is a public and global communication tool and that any content posted may reflect on the school, its reputation and services.

2. I will not use the site or group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the headteacher. The headteacher retains the right to remove or approve content posted on behalf of the school.

4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
    - Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices.Images taken for the sole purpose of inclusion on Facebook will not be forwarded to any other person or organisation.

6. I will promote online safety in the use of Facebook and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the headteacher prior to use.

7. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The headteacher will have full admin rights to the site.

8. Where it believes unauthorised and/or inappropriate use of Facebook or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the headteacher urgently.

11. I will ensure that the Facebook page is moderated on a regular basis as agreed with the headteacher.

12. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

13. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the headteacher.

I have read, understood and agree to comply with the Rusthall St Paul's Social Networking Acceptable Use policy.

Signed: ……………………….... Print Name: ……………………… Date: ………Accepted by: ……………………………. Print Name: ………………………….