Online Safety Policy

Lead Person: Mike Mitchell

Policy Date: November

2022 Review Date:

November 2022

Chair of Governors *C Stunell*

Headteacher *M Mitchell*

Contents

Seven Stars Primary School Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Seven Stars Primary School involving staff, pupils and parents/carers, building on the Lancashire County Council (LCC) safeguarding policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2021, Early Years and Foundation Stage and the Lancashire Safeguarding Board
- Seven Stars Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile technology or social media.
- The purpose of Seven Stars Primary School online safety policy is to:
    - Safeguard and promote the welfare of all members of the school when online and using mobile devices or social media.
    - 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.
- Seven Stars Primary School 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

- Online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online including social media and mobile technology.
- Seven Stars Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and that pupils should be empowered to build resilience and to develop 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
  - Code of conduct for parents, visitors, staff and volunteers
  - Behaviour and Relationships Policy
  - Safeguarding and Child Protection Policy
  - Curriculum policies, such as:
    - Computing
    - Personal Social and Health Education
  - Data Protection-GDPR Policy
  - SEND Policy
  - Whistleblowing Policy

3. Monitoring and Review

- Seven Stars Primary School will review this policy and practices at least annually and also following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use; pupil's internet use will be monitored through teacher and teaching assistants whilst in their care, staff's internet use will be monitored through the filtering system and will be investigated further should anything be flagged up.
- We will evaluate online safety mechanisms to ensure that this policy is consistently applied.
- The DSL team will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis 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

- Mike Mitchell (Head teacher) is the DSL who is Online Safety Lead at Seven Stars Primary School.
- Seven Stars Primary School recognises that all members of the community have important roles and responsibilities with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and an Acceptable Use Agreement, which covers acceptable use of technology. Ensure that suitable and appropriate filtering and monitoring systems are in place.

- Work with technical staff and providers to monitor the safety and security of school systems and networks.
- 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. (KCSIE 2021 Appendix D p150)
- Support the Online Safety Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Team will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- 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.
- 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 schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, 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 for safeguarding and online safety.

4.3 Members of staff will:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and Acceptable Use Agreement
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education within the curriculum.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online 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 signposting 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)* 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 is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

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 appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school Acceptable Use Agreement
- 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 there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the school Acceptable Use Agreements and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and Acceptable Use Agreement. 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.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- 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 Education and engagement with pupils

- The schools will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, RSHE and Computing programmes of study, covering use both at home school and home. (e.g. Friendship/Respect week, Safer Internet Day, regular focus on online safety)
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by pupils.
    - Implementing appropriate peer education approaches.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

5.1.1 Vulnerable Pupils

- Seven Stars Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, 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.
- Seven Stars Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils (see also SEND policy).
- Seven Stars Primary School will seek input from specialist staff as appropriate, including the Inclusion Lead, staff with pastoral responsibilities and the SLT.

5.2 Training and engagement with staff

Seven Stars 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 staff on a regular basis, with at least annual updates.
    - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- 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 within school.
- 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

- Seven Stars Primary School 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 will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
    - Requiring them to read the school Acceptable Use Agreement and discuss its implications with their children.

6. Reducing Online Risks

- Seven Stars Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
    - 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, using guidance from UK Safer Internet Centre and KCSIE 2021 Appendix D
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and 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

- Seven Stars 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
    - School learning platform/intranet
    - Email
    - Games consoles and other games based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place. This will be done through education of the children, filters that are in place and careful supervision whilst they are being used. This use must also be in class time only. It will be the responsibility of the member of staff who has planned for children to use devices, to ensure that the school guidelines are strictly followed.
- 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 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 a record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making (KCSIE 2021)

- Seven Stars Primary School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks via Netsweeper filtering
- The governors and leaders are 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.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- 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:
    - BTLancs
- The school's filtering systems blocks all sites on the Internet Watch Foundation (IWF) list, which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- https://www.netsweeper.com/education/
- The school works with their respective providers to ensure that our filtering policy is continually reviewed and is in line with UK Safer Internet Centre and KCSIE 2021:

7.3.3 Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to a member of the Designated Safeguarding Team.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Lancashire Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring and supervision of the children using the devices
    - Monitoring internet and web access through the technology monitoring services provided by: https://www.netsweeper.com/education/
- The school has a clear procedure for responding to concerns identified via monitoring approaches. Issues should be raised and will be responded to, by following the Child Protection procedures that are already in place.
- 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 the GDPR -Data Protection Act 2018.
    - Full information can be found in the school's Data protection-GDPR Policy.

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 schools' networks.
    - The appropriate use of user logins and passwords to access the school networks.
    - 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.
- We require all users to:
    - Use strong passwords for access into our system.
    - 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.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- 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's website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school websites 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): Image Use Policy, Data Protection-GDPR Policy, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones-see Annexe.

7.8 Managing Email

- Access to school's email systems will always take place in accordance with Data 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 contains sensitive 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.
    - Email access on personal devices should be through the Outlook App and should require touch id or face recognition.
- Members of the school community will immediately tell the DSL Team 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.

7.8.1 Staff

- 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 school 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 parents.

7.8.2 Pupils

- Pupils will use school provided email accounts for educational purposes. Parents will be asked to provide consent should there be an educational requirement.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- Seven Stars Primary School recognises that video conferencing or use of webcams can bring a wide range of learning benefits.
    - All videoconferencing or webcam 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 point to point encrypted connections. Our IP address is not made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - 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 external videoconferencing activities.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- 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 Applications (Apps) used to Record Children's Progress

- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems via Apps is appropriately risk assessed prior to use, and that they are used in accordance with 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 Seven Stars Primary School 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 Seven Stars Primary School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of Seven Stars Primary School 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.
    - The use of social media during school hours for personal use is not permitted.
    - 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 Seven Stars Primary School community on social media, should be reported to the school and will be managed in accordance with our Whistleblowing, Anti-bullying, Behaviour, Rewards and Sanctions and Child Protection policies.

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 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 the AUP.

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.
    - 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 Seven Stars Primary School 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's 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.

8.2.3 Communicating with pupils and parents and carers

- 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.
- 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 Designated Safeguarding Lead and/or the headteacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Learners use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- 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. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Learners 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 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.
  - 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 learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to online safety 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 learners as appropriate, in line with our behaviour policy. Civil or legal action will be taken if necessary.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8.4 Official use of social media

- Official social media channels are:
  - Seven Stars Facebook Page Seven Stars Facebook Page
- The official use of social media sites by Seven Stars Primary school only takes place with clear educational or community engagement objectives and with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
- 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 channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
- Staff managing official social media channels will use school provided email.
- Teachers can access Facebook via the 'Administrator' or can upload/post via their own personal account

- Official social media sites are suitably protected and, where possible, are linked to our website.
- Public communications on behalf of the setting 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 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.
- Parents/carers and learners 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 tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will try to 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 participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - 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.
    - Ensure appropriate consent has been given before sharing images on the official social media channel.
    - 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/direct messaging with current or past learners or parents/carers.
    - Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Personal Devices and Mobile Phones

- Seven Stars Primary School 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 mobile technology including mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology (including 'smart watches' and fitness trackers which facilitate communication or have the capability to record sound or imagery) will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and 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 Seven Stars Primary School 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 Seven Stars Primary School 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 toilets or when children are not dressed, etc.
- 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 our Conduct policy.
- All members of Seven Stars Primary School 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 school Behaviour or Child protection policies.

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
    - 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 use personal devices during teaching periods, unless written permission 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 undermine this, will be discussed with the Designated Safeguarding Lead.
- 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.
    - 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 Conduct 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.

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.
- Seven Stars Primary School expects pupil's personal devices and mobile phones to be kept in a secure place designated by the school and switched off.
- Mobile phones or personal devices will not be used by pupils at any time during the school day.
- 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 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 DFE's Searching, Screening, Confiscation Guidance
    - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of a parent/ carer following the DFE's Searching, Screening, Confiscation Guidance
    - Mobile phones and devices that have been confiscated will be released to parents or carers.
    - 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) 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. Code of Conduct
- 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 policy breaches

- All members of the community will be made aware of how Seven Stars Primary School will monitor policy compliance eg: AUPs, staff training, classroom management
- All members of the community are informed of the need to report policy breaches or concerns in line with existing policies, including those mentioned in section 2.2**.**
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- If appropriate, after any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from relevant agencies in accordance with our Safeguarding and child protection policy.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Lancashire Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher according to the Whistleblowing Policy
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- The school will follow the advice as set out in the non-statutory
    - UKCCIS guidance: 'Sexting in Schools and Colleges UKCCIS'
- Seven Stars Primary School 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.
- Seven Stars Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

- 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 our **Child protection and Safeguarding policies** and the relevant Lancashire Safeguarding Child Board's procedures:
    - Initial Response
        - The incident should be referred to the DSL as soon as possible
        - The DSL should hold an initial review meeting with appropriate school staff to establish the facts and assess the risks
        - There should be subsequent interviews with the young people involved (if appropriate)
        - Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
        - At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.
- The DSL will follow the guidance from UKCCIS: 'Sexting in Schools and Colleges UKCCIS' with regards to the following actions:
    - Securing and handing over devices to the police
    - Searching devices, viewing and deleting imagery
    - Interviewing and talking to the young person/people involved
    - Recording incidents

11.2 Online Child Sexual Abuse and Exploitation

- Seven Stars Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Seven Stars Primary School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse 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 sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community through the school's website

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- 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. Lancashire Safeguarding Children Multi-Agency Partnership
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Lancashire 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.
    - Make a referral to Specialist Children's Services (if required/ 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 take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
    - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via CEOP
- If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Lancashire Safeguarding Team and/or Lancashire 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 Lancashire Safeguarding team by the Designated Safeguarding Lead.

- If pupils at other schools are believed to have been targeted, the school will seek support from Lancashire Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- Seven Stars Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 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 IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation 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 Lancashire Police and/or the Lancashire Education Safeguarding Service

- If made aware of IIOC, the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Lancashire Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Lancashire 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 .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - 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.
    - 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.

12 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Seven Stars Primary School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

13 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Seven Stars Primary School and will be responded to in line with existing school policies, including 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, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Lancashire Safeguarding team and/or Lancashire Police.

14 Online Radicalisation and Extremism

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the 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 protection policy.
- If the 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 Whistleblowing policies.

Seven Stars Primary School Pupil Acceptable Use Policy

Dear Child

All pupils at our school use computer facilities including internet access as an essential part of learning and fun in today's modern British Society. You will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines, social media and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

At Seven Stars Primary School we recognise the essential and important contribution that technology plays in promoting your learning and development, both at school and at home. However we also recognise there are potential risks involved when using online technology. The school will take all reasonable precautions to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online.

At Seven Stars Primary School we want to ensure that all members of our community are safe and responsible uses of technology. We will support you to:

- Become empowered and responsible digital creators and users.
- Use our school resources and technology safely, carefully and responsibly.
- Be kind online and help us to create a school community that is respectful and caring, online and offline.
- Be safe and be sensible online and always know that you can talk to a trusted adult if you need help.

We request that you and your family read the school Acceptable Use Policy and return the attached slip.

Should you have any worries about online safety then you can speak with your class teacher, or any other adult in the school. You can also access support via other websites such as www.thinkuknow.co.uk and www.childline.org.uk.

We look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,

Mike Mitchell

Headteacher

Seven Stars Primary KS1 Pupil Acceptable Use Policy Agreement Form

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe online.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online.
- I follow the rules when using all the ICT equipment in school.
- I know that if I do not follow the rules then I know the school behaviour system will be used.
- I have read and talked about these rules with my parents/carers.
- I always tell an adult/teacher if something online makes me feel unhappy or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

Seven Stars Primary School
KS1 Pupil Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the pupil Acceptable Use Policy (AUP).

I agree to follow the pupil AUP when:

1. I use school systems and devices, both on and offsite.
2. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website.

Name……. Signed……..

Class…… Date……..

Parents Name..... Parents

Signature…….

Date…….

Seven Stars Primary KS2 Pupil Acceptable Use Policy Agreement Form

Safe

- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are appropriate and if I have permission.
- I only talk with and open messages from people I know and I only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Trust

- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, image or text I use.

Responsible

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school computers for school work, unless I have permission otherwise.
- I follow the rules for using any piece of ICT equipment in school.
- I know I can only bring my own devices into school with the school's permission and I will follow the instructions and guidance of use as instructed by the school.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.
- I will only change the settings on the computer if a teacher/technician has allowed me to.

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules then I know the school behaviour system will be used.

Tell

- If I am aware of anyone being unsafe with technology then I will report it to a teacher.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.

Seven Stars Primary School
KS2 Pupil Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the pupil Acceptable Use Policy (AUP).

I agree to follow the pupil AUP when:

1. I use school systems and devices, both on and offsite.
2. I know I can only bring my own devices into school with the school's permission and I will follow the instructions and guidance of use as instructed by the school.
3. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website.

Name……. Signed……..

Class…… Date……..

Parents Name..... Parents

Signature…….

Date…….

Seven Stars Primary Parent/Carer Acceptable Use Policy

Dear Parent/Carer

All pupils at Seven Stars Primary School use computer facilities and internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Mobile Phones

Seven Stars Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development, believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks.
We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip.

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website Seven Stars Primary School for more information about our approach to online safety. Full details of the school's online safety policy are available on the school website or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the school Online Safety Lead (Mike Mitchell) or the Designated Safeguarding Lead (Deborah Wright).

Yours sincerely,

Mike Mitchell

Headteacher

Seven Stars Primary School Parent/Carers Acceptable Use Policy

1. I have read and discussed Seven Stars Primary School Pupil Acceptable Use Policy with my child.
2. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, in order to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, rewards and sanctions, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted.
7. I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
8. I know that I can speak to the school Online Safety Lead (Mike Mitchell/Cathy Walsh), Designated Safeguarding Lead (Deborah Wright), my child's teacher or any other member of leadership if I have any concerns about online safety.
9. I will visit the school website Seven Stars Primary School for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:
    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com
11. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I have read, understood and agree to comply with Seven Stars Primary School's Parent/Carer Acceptable Use Policy.

Child's Name…… Class…….

Parents Name…….....Parents Signature…….

Seven Stars Primary School Staff Acceptable Use Policy

Dear

At Seven Stars Primary School we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at Seven Stars Primary School take precautions in order to protect themselves both professionally and personally online. With this in mind, we request that all members of staff:

- Are conscious of their own professional reputation and that of the school when online.
  - All members of staff are strongly advised in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
  - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This can have consequences including civil, legal and disciplinary action being taken.

- Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute, and does not undermine professional confidence in our abilities.
  - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.

- All Staff be careful when publishing any information, personal contact details, video or images online.
  - It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online, but do so respectfully.
  - Ensure that the privacy settings of the social media sites that you use are set appropriately and access to restricted
  - Ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all.

- Do not to accept pupils (past or present) or their parents/carers as "friends" on a personal account.
  - You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
  - If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns, please speak to the Designated Safeguarding Lead (Deborah Wright/Mike Mitchell).

- Always use a work provided email address or phone number to contact children and parents – this is essential in order to protect yourself as well as the wider community.

- If you are concerned about a child's wellbeing or online behaviour then please speak to the Designated Safeguarding Lead. If you are targeted online by a member of the community or are concerned about a colleague, then please speak to the Headteacher and/or chair of governors.
    - If you are unhappy with the response you receive, or do not feel able to speak to the Designated Safeguarding Lead, Headteacher, or chair of governors then we request you follow our Whistleblowing procedure.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" are available to help you consider how to protect yourself online.

Please download the documents directly from:

- www.childnet.com,
- www.e-safety.org.uk
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk

Additional advice and guidance for professionals is available locally through the Education Safeguarding Team or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to your line manager or the Designated Safeguarding Lead if you have any queries or concerns regarding this.

Yours sincerely,

Mike Mitchell

Headteacher

Seven Stars Primary School Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Seven Stars Primary School's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand the School's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school/setting systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within the School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies**.**

2. I understand that Seven Stars Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the School's staff behaviour policy/code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school/setting ethos, school/setting staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School/Setting Devices and Systems

4. I will only use the equipment and internet services provided to me by the school/setting for example school/setting provided laptops, tablets, mobile phones and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    a. I will use a 'strong' password to access school/setting systems.
    b. I will protect the devices in my care from unapproved access or theft.

7. I will respect school/setting system security and will not disclose my password or security information to others.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the Headteacher

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the Head of School.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the School's information security policies.
    a. 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.
    b. Any data being removed from the school's site, such as via email will be suitably protected. This may include data being encrypted by a method approved by the school/setting. Memory Sticks will not be used to transport data out of school.

11. I will not keep 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's learning platform to upload any work documents and files in a password protected environment. (Microsoft Office 365)

12. I will not store any personal information on the school's IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

13. I will ensure that the School owned information systems are used lawfully and 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.

14. I will not attempt to bypass any filtering and/or security systems put in place by the School.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider (BT Lancs) as soon as possible.

16. If I have lost any School related documents or files, I will report this to the ICT Support Provider and school's Data Protection Officer (Jennifer Pullin) as soon as possible.

17. Any images or videos of learners will only be used as stated in the school/setting camera and image use policy.

a. I understand images of learners must always be appropriate and should only be taken with School provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of learners, as outlined in Seven Stars Primary School online safety policy.

19. I have read and understood Seven Stars Primary School online safety policy which covers expectations for learners regarding mobile technology and social media.

20. I will promote online safety with the learners 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 by:
    a. exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    b. creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    c. involving the Designated Safeguarding Lead (DSL) or DDSL as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    d. make informed decisions to ensure any online safety resources used with learners is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school/setting online safety/child protection policy.

22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

1. I have read and understood the school/setting online safety policy which covers expectations regarding staff use of mobile technology and social media.

2. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy/code of conduct, when using school/setting and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    - I will take appropriate steps to protect myself online when using social media as outlined in the online safety/social media policy.
    - I am aware of the school/setting expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety policy.
    - I will not discuss or share data or information relating to learners, staff, Seven Stars Primary School business or parents/carers on social media.

- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with Seven Stars Primary School code of conduct and the law.

3. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via Seven Stars Primary School approved and provided communication channels, such as Seven Stars Primary School email address or telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
    - If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the Headteacher.

4. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the Headteacher.

5. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

6. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

7. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school/setting into disrepute.

Policy Compliance

8. I understand that the school/setting may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

9. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school/setting online safety/child protection policy.

10. I will report concerns about the welfare, safety or behaviour of staff to the Headteacher, in line with the whistleblowing policy.

11. I understand that if Seven Stars Primary School believe that unauthorised and/or inappropriate use of Seven Stars Primary School systems or devices is taking place, Seven Stars Primary School may invoke its disciplinary procedures as outlined in the staff code of conduct.

12. I understand that if Seven Stars Primary School believe that unprofessional or inappropriate online activity, including behaviour which could bring the School into disrepute, is taking place online, the School may invoke its disciplinary procedures as outlined in the staff code of conduct.

13. I understand that if Seven Stars Primary School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Seven Stars Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: …….....

Date (DDMMYY)……...

Seven Stars Primary School Visitor and Volunteer
Acceptable Use of Technology Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUP will help Seven Stars Primary School ensure that all visitors and volunteers understand the School's expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Seven Stars Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and communication technologies**.**

2. I understand that Visitor and Volunteer AUP should be read and followed in line with Seven Stars Primary School code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school/setting ethos, Seven Stars Primary School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am allowed to take images or videos of learners. Any images or videos of learners will only be taken in line with the School's camera and image use policy.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners, as outlined in Seven Stars Primary School online safety policy.

7. I will support teachers in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

8. I will immediately report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the Designated Safeguarding Lead (DSL) (Deborah Wright/Mike Mitchell) in line with Seven Stars Primary School online safety/child protection policy.

9. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content if videos, images, text or music is protected, I will not copy, share or distribute or use it.

Seven Stars Primary School Staff Acceptable Use of

Social Media and Mobile Technology Policy

1. I have read and understood Seven Stars Primary School online safety policy which covers expectations regarding staff use of social media and mobile technology.

2. I will ensure that my online reputation and use of technology and is compatible with my role within Seven Stars Primary School. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the online safety policy.
    - I will not discuss or share data or information relating to learners, staff, school, business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with Seven Stars Primary School code of conduct and the law.

3. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL (Deborah Wright/Cathy Walsh) or the Headteacher.

4. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL (Deborah Wright/Cathy Walsh) or the Headteacher.

5. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

6. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

7. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of Seven Stars Primary School into disrepute.

Policy Compliance, Breaches or Concerns

8. I understand that the School may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

9. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with Seven Stars Primary School child protection policy.

10. I will report concerns about the welfare, safety or behaviour of staff to the head of school, in line with the whistleblowing policy.

11. I understand that if Seven Stars Primary School believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the School may invoke its disciplinary procedures.

12. I understand that if the School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Seven Stars Primary School Acceptable Use of Social Media and Mobile Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……

Signed: …….....

Date (DDMMYY)……...

Seven Stars Primary School Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of Seven Stars Primary School community are fully aware of the School's boundaries and requirements when using the school/setting 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/setting community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. Seven Stars Primary School provides Wi-Fi for the School's staff and allows access for education use only.

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 technology falls under Seven Stars Primary School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy, data protection policy and child protection policy, which all learners/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; 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 school's 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 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. I confirm that I knowingly assume such risk.

8. Seven Stars Primary School accepts no responsibility for any software downloaded and/or installed, email 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/setting from any such damage.

9. Seven Stars Primary School accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school/setting wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, 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 School's security and filtering systems or download any unauthorised software or applications.

12. My use of Seven Stars Primary School's Wi-Fi will be safe and responsible and will always be in accordance with the School's 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 or inappropriate 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 Lead as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the DDSL.

16. I understand that my use of the School's Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the School may 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 agreed to comply with Seven Stars Primary School Wi-Fi acceptable Use Policy.

Name ……...

Signed: …….....Date (DDMMYY)……