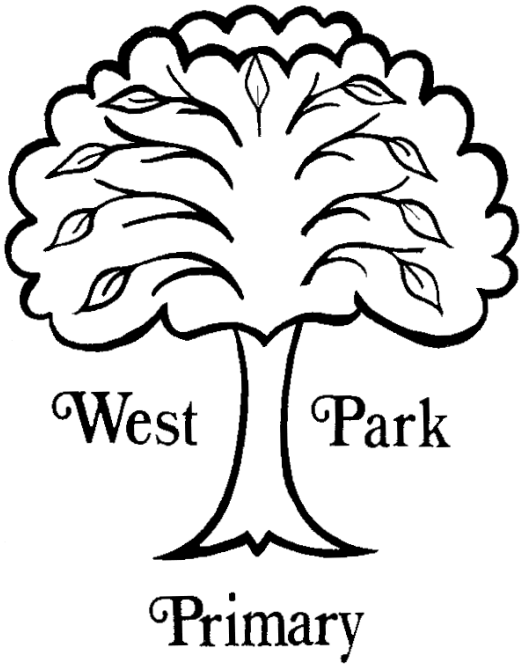
West Park Primary School



Respect Aspiration Resilience Integrity

Online Safety Policy

Contents

Online Safety Policy Template Content

West Park Primary School Online Safety Policy

1. Policy aims

- This online safety policy has been written by West Park Primary School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice from Online Behaviours Ltd.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' and DfE 'Safeguarding and remote education during coronavirus (COVID-19)'
- This policy should also be read in conjunction with Ofsted's 'Review of sexual abuse in schools and colleges' and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- West Park Primary School is currently operating in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) 2021 and related guidance, however, remain the same.
    - Where children are asked to learn online at home in response to a full or partial closure, West Park Primary School will follow expectations as set out within the Safeguarding & Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.

- The purpose of West Park Primary School's online safety policy is to
    - safeguard and promote the welfare of all members of West Park Primary School community online.
    - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.

- West Park Primary School identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk, as identified in KCSIE 2021.
    - **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.
    - **Commercial:** risks such as: online gambling, access to inappropriate advertising, phishing, in-game purchasing and or financial scams

2. Policy scope

- West Park 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 online.
- West Park 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 which present positive and exciting opportunities, as well as challenges and risks.
- West Park Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as learners and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
    - Behaviour and discipline policy
    - Child protection policy & Safeguarding
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security
    - Searching, screening and confiscation policy

3. Monitoring and review

- Technology evolves and changes rapidly; as such West Park Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Deputy Head Azizan Kabil is recognised as leading Online Safety and Elaine Dovydaitis as holding overall lead responsibility for online safety, in line with KCSIE 2021.
- West Park Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team, supported by the Online Safety Lead (OSL) will:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) supported by the OSL will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.

- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- 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 settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the school 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 (ideally termly) with the governor with a lead responsibility for safeguarding/online safety.

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

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

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

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as social media platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school delivery is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework 2020' and DfE 'Teaching online safety in school' guidance.
    - Delivering an online safety curriculum using Project Evolve, supported by our RSHE curriculum and Elim ActiveBytes
    - ensuring online safety is addressed, where appropriate, within Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - implementing appropriate peer education approaches such as Digital Leaders or Digital Ambassadors.
    - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our learners.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
    - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments if appropriate.

- West Park Primary School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
    - displaying acceptable use posters in all rooms.
    - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
    - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- West Park Primary School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.

- teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation as well as how to avoid infringing copyright and plagiarism.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- West Park Primary School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- West Park Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at West Park Primary School will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will
  - provide and discuss the online safety policy, AUPs and procedures with all members of staff as part of induction.
  - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be achieved via:
    - Annual safeguarding training
    - Annual online safety briefing
    - Ongoing professional development such as EPICT
    - Regularly as part of staff meetings
    - Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
  - build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.

- make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- West Park Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We 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:
    - Specific online safety briefings
    - Parent/carer workshops/accreditation
    - Newsletters
    - The school website and social media channels
    - Parents' evenings
  - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

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

- We will
  - regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- All members of the community are made aware of our 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. This is clearly outlined in our

acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- West Park 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
  - Teams
  - Email
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
  - All staff laptops and external hard drives are encrypted
  - All iPads are managed using device management software to allow remote wiping, locking and location detection. Pupils cannot install or delete apps. All iPads are numbered, and children are allocated certain ones. Pupil content is wiped from devices regularly.
- Members of staff will always evaluate websites, (particularly YouTube – https://safeyoutube.net/ or https://safeshare.tv will be used to ensure a safe experience), tools and apps fully before use in the classroom or recommending for use at home. New apps will only be allowed following a suitable risk assessment.
- The setting will use appropriate search tools as identified following an informed risk assessment. **SWGfL Swiggle** will be used as the default search engine up to and including Year 4. Other search engines may be used in years 5 & 6 with appropriate safe searching activated as default, once pupils have been shown how to search safely and how to report any concerning search results.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems, including Wi-Fi.

- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

7.3 Filtering and monitoring

7.3.1 Decision making

- West Park Primary School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- 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.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- West Park Primary School's education broadband connectivity is provided through Wolverhampton City Council
- West Park Primary School uses using light speed solutions
    - using light speed solutions blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - using light speed solutions is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
- We work with Wolverhampton City Council to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to:
    - turn off monitor/screen
    - report the concern immediately to a member of staff who will report the URL of the site to technical staff/services.
    - Staff may wish to record this as a safeguarding issue depending on the circumstances
- Filtering breaches will be reported to the OSL and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners **as appropriate.**
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - e.g. physical monitoring (supervision)
    - monitoring internet and web access (reviewing logfile information)
    - Senso - active/pro-active technology monitoring services.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches, we will respond swiftly in line with the safeguarding & child protection policy.

7.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our information security policy which can be accessed at (*Link or location*). **awaiting update from Chris Watabiki**

7.5 Security and management of information systems

- We take 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 eg memory sticks/external storage devices.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments. Included in AUP for staff
    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools eg staff will not disable proxy settings whilst in school or link to mobile phones
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- In KS2 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system.
    - Alert the OSL if they suspect it has been compromised.

- not share passwords or login information with others or leave passwords/login details where others can find them.
- not to login as another user at any time.
- lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE https://www.gov.uk/guidance/what-maintained-schools-must-publish-online or
- We 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 learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Use of images and videos, including online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) data security, acceptable use policies, codes of conduct/behaviour, (use on social media and use of mobile devices is covered later).
- Written permission from parents or carers (and learners where possible) will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, **the personal equipment of staff should never be used for such purposes.**
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. Staff should only use recognised school email systems in relation to work.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the Headteacher/DSL/OSL if they receive offensive communication, and this will be recorded in our 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 on site.

7.8.1 Staff email

- All members of staff are provided with an 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. Staff are not expected to respond to emails late in the evening, unless in an emergency.

7.8.2 Learner email

- Learners will use a school provided Microsoft account for educational purpose. Access to emails is restricted unless there is a requirement for an educational purpose.
- Learners will discuss and agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Staff emails will be used for communication outside of the setting eg with an author or external organisation.

7.9 Remote/ online learning

- This section links to the school's Remote Learning plan and AUPs specific to remote learning
- West Park Primary School uses a range of online learning resources, all of which have been risk assessed before being made available to learners.
- Microsoft Teams is used as the school's online learning environment. All users discuss and agree the school's AUP before use as well as the platform specific AUP to ensure expectations are known and safety is maintained. (to see the AUP in detail, click here).
- Parents/carers will be informed about the use of the learning environment and encouraged to support their child in contributing positively and reporting issues should they occur.
- Staff should also be aware of their role in maintaining a professional online environment.
- Should any member of staff wish to conduct a 'live' video lesson at any time (eg where remote learning activities are required for all or some pupils due to Covid-19), this should be discussed with senior leaders/DSL/OSL to ensure the correct systems are put in place (to

see these processes in detail, please see the AUP and Remote Learning Plan). Multiple adults are required for any on line 1-1 activity add to staff acceptable use policy
- Systems are in place to ensure the correct pupils have access and other pupils cannot join teams/classes without being added by members of staff.
- Leaders and staff will regularly monitor the use of Teams to ensure appropriate and safe use. Any incidents will be reported immediately and dealt with in line with school behaviour/safeguarding & child protection policies. Any abusive/ inappropriate content will be removed immediately, and the following sanctions may apply:
    - Access for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing safeguarding and child protection procedures.

7.10 Management of applications (apps) used to record children's progress

We use SIMs to track learners progress and share appropriate information with parents and carers.

- The Headteacher/OSL will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
    - only learner issued devices will be used for apps that record and store learners' 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 learners' personal details, attainment or images.
    - 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 West Park 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 West Park Primary School community are expected to engage in social media in a positive and responsible manner.
    - All members of West Park Primary School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school provided devices and systems on site.
    - Pupils cannot access social media using school devices or whilst connected to school Wi-Fi. Selected staff may be given access on school devices eg to Twitter/Facebook to allow updating of the school's official social media channels.
    - The use of social media during school hours for personal use is not permitted for learners.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.
- Concerns regarding the online conduct of any member of West Park Primary School community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and safeguarding & child protection policies.

8.2 Staff personal use of social media

- The safe and responsible use of social media 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 our code of conduct/behaviour policy and/or acceptable use of technology policy.

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 the school.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. 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 appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.

- Members of staff are encouraged not to identify themselves as employees of West Park Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners 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.

8.2.2 Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with, or add, any current or past learners or their family members as 'friends' on any personal social media sites.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the headteacher.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.
- Any communication from learners and parents received on personal social media accounts will be reported to the Deputy Head, DSL (or deputy) and/or the headteacher.

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.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- 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.
- 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.

8.4 Official use of social media

- West Park Primary School official social media channels are:
  - *Twitter link; @westparkpri*
- The official use of social media sites by West Park 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 use school provided email addresses to register for and manage official social media channels.
  - Official social media sites are suitably protected
  - 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.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

8.4.1 Staff expectations

- Staff are discouraged from liking or commenting on posts from the official school social media using their personal accounts as this might make them visible to parents and pupils.
- 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. Mobile Technology: Use of Personal Devices and Mobile Phones

- West Park Primary School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of West Park Primary School community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of West Park 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 site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of West Park Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our 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 policy and procedures, such as confidentiality, child protection, data security and acceptable use of technology.
- Staff will be advised to:
    - keep mobile phones and personal devices in a safe and secure place (e.g. locked in a locker/drawer) 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 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.
- Staff will only use school provided equipment (not personal devices):
    - to take photos or videos of learners in line with our image use policy.
    - to work directly with learners during lessons/educational activities
    - to communicate with parents and carers.
- Where remote learning activities are required because of Covid-19, staff will use school provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.3 Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - Mobile phones may only be brought to school with prior permission
    - West Park Primary School expects learners' personal devices and mobile phones to be handed in the school office on arrival and collected at the end of the day.
    - When learners attend an after-school club, mobile devices should once again be handed in at the beginning of the session and collected at the end.
- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, online safety, behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy and in line with the DfE 'Searching, Screening and Confiscation' guidance.

- Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the day (week, term etc)
- If there is suspicion that material on a learner'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

- All visitors/contractors will leave their phone in their pocket and turned to silent. If required to take a call, visitors must move to an agreed area free from children.
- Under no circumstances will it be used (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students.
- If required (e.g. to take photos of equipment or buildings), visitors will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- 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 inform the DSL (or deputy) or Headteacher of any breaches of our policy.

10. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community 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 online safety issues.
- 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 the Education Safeguarding Service.
- 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 as appropriate.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL and/or Headteacher will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- West Park Primary School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the headteacher, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy/code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or deputy).The Headteacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Child on child sexual violence and sexual harassment

- Our headteacher, DSL and appropriate members of staff have accessed and understood Ofsted's 'Review of sexual abuse in schools and colleges' (2021) recommendations and part 5 of 'Keeping Children Safe in Education' 2021
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our safeguarding & child protection policy.
- We take the view that **'it could happen here'** and recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - Non-consensual sharing of sexual images and videos
    - Sexualised online bullying
    - Online coercion and threats
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
    - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - if content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice and policy.
    - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - implement appropriate sanctions in accordance with our behaviour policy.
    - inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
    - if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
    - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- West Park Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

- West Park Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, West Park Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- West Park Primary School recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
    - We will follow the advice as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes Advice for education settings working with children and young people Responding to incidents and safeguarding children and young people.
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- West Park Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery eg the school website, internal platforms, staff room.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - act in accordance with our child protection policies and the relevant local procedures.

- ensure the DSL (or deputy) responds in line with the UKCIS guidance.
- Store any devices containing potential youth produced sexual imagery securely
  - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS guidance.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
  - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- West Park Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- West Park Primary School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community – this can be accessed on the school website here.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
  - act in accordance with our child protection policies and the relevant local procedures.

    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- West Park Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:

    - act in accordance with our child protection policy and the relevant WST procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 setting provided devices, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - ensure that the Headteacher is informed in line with our managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
    - quarantine any devices until police advice has been sought.

11.5 Online bullying

- Online bullying, along with all other forms of bullying, will not be tolerated at West Park Primary School.
- Full details of how we will respond to online bullying are set out in our anti-bullying policy.

https://cloudw.sharepoint.com/:w:/r/sites/schools/2116/staff/_layouts/15/Doc.aspx?sourcedoc=%7B00C2A4AA-21F9-4D7F-A722-F2E70DCDC4A7%7D&file=Anti-bullying%20Policy%202020.docx&action=default&mobileredirect=true

11.6 Online hate

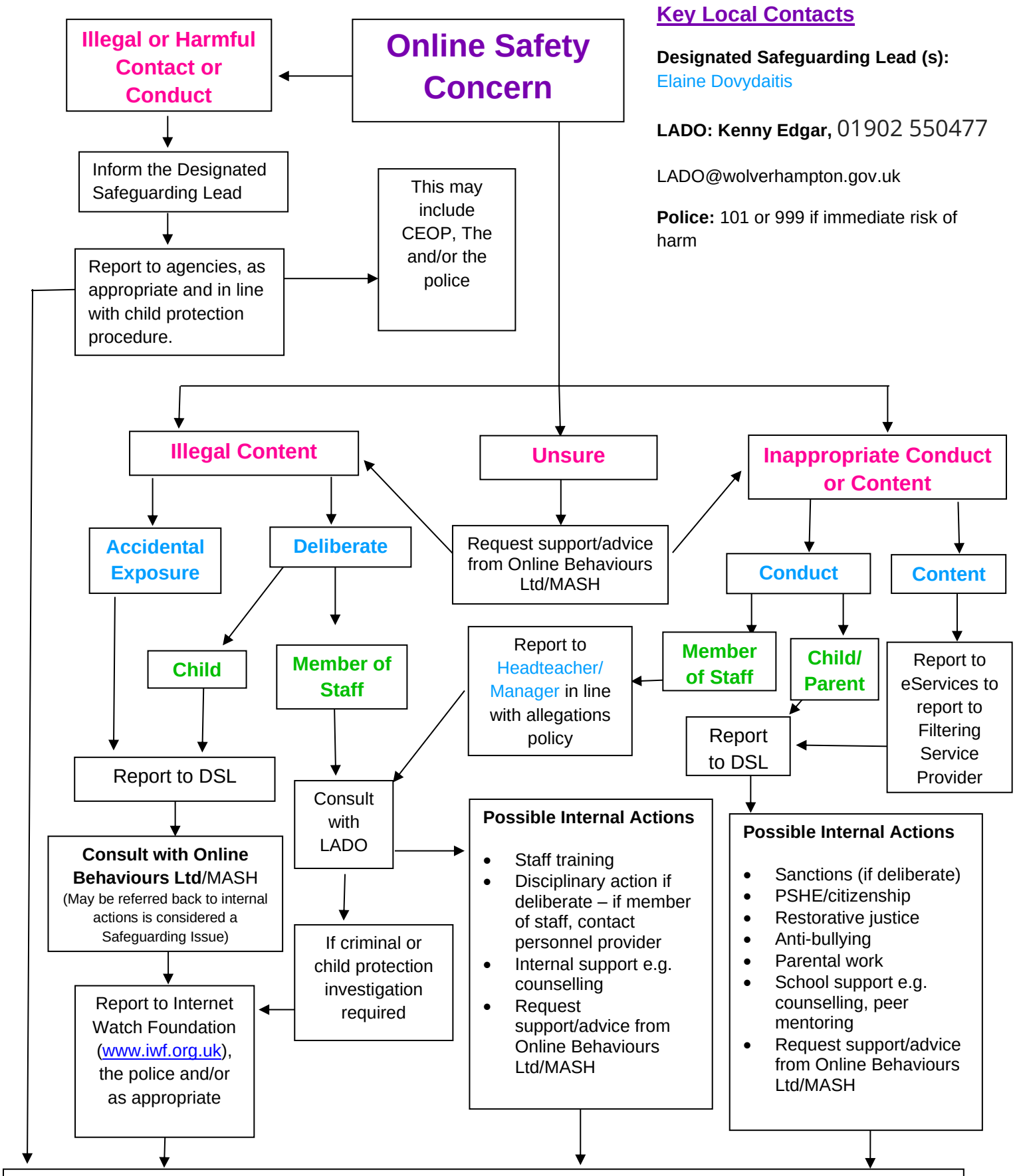
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at West Park Primary School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Responding to an Online Safety Concern Flowchart



National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

Acceptable Use Policy (AUP) for STAFF & VOLUNTEERS

What am I agreeing to?

1. I have read and understood West Park Primary School's full Online Safety policy https://www.westparkprimaryschool.co.uk/policies and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult). Azizan Kabil/Briony Jones.
3. **During remote learning:**
    - I will have read, understood and signed the AUP for remote learning
    - **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
    - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
    - **I will not take recordings or screenshots** of myself or pupils during live lessons.
    - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    - **I will complete the issue log for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students
4. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
5. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum,** as well as safeguarding considerations when supporting pupils remotely.
6. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

7. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
8. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. https://www.westparkprimaryschool.co.uk/policies I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
10. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in West Park's social media policy/guidance
11. I agree to adhere to all provisions of the school Data Protection Policy https://www.westparkprimaryschool.co.uk/policies at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify Azizan Kabil/Briony Jones, if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
12. I will not store school-related data on personal devices, storage or cloud platforms. I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
13. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
14. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
15. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
16. I will follow the guidance in the safeguarding and online safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here https://www.westparkprimaryschool.co.uk/policies may lead to appropriate staff disciplinary action

or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

Acceptable Use Policy (AUP) for KS2 PUPILS

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I can't go to school because of coronavirus*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

15. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable, particularly 18+ games which are extremely unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever, even if I delete it.
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

If I have any questions, I will speak to a trusted adult:

In school that includes _____

Outside school, my trusted adults are _____

Signed: _____ **Date: _____**

For parents/carers

If your parents/carers want to find out more, they can read West Park Primary School's full Online Safety Policy https://www.westparkprimaryschool.co.uk/policies

West Park Primary

Respect-Aspiration-Resilience-Integrity

Acceptable Use Policy (AUP) for KS1 PUPILS

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:	✓
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

For parents/carers

To find out more about online safety, you can read West Park Primary School's full Online Safety Policy