West Park Primary School

Online Safety Policy

Respect Aspiration Resilience Integrity

Adopted by: West Park Primary School

On: 26.9.23

Signed (Chair of Governors):

Minute number:

Contents

Responding to an Online Safety Concern Flowchart
Acceptable Use Policy (AUP) for STAFF & VOLUNTEERS
Acceptable Use Policy (AUP) for KS2 Pupils
Acceptable Use Policy (AUP) for KS1 Pupils
MyConcern Reporting Guidance

Policy Aims

Our school aims to:

- Have robust systems in place to ensure the online safety of pupils, staff volunteers and governors.
- Identify and support families that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in the online world.
- Enable all staff to work safely and responsibly, model positive online behaviours and manage professional standards and practices when using technology.
- Identify clear procedures to follow when responding to online safety concerns.

The 4 key categories of risk
Our approach to online safety is based on addressing the following risk categories:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

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

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.

Roles and Responsibilities

1.1. The Headteacher Azizan Kabil (DSL)

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The headteacher has overall lead responsibility for online safety, inline with KCSiE.

1.2. The Online Safety Lead Sarah Andrews (Deputy Headteacher and DDSL) will:

- Create a whole school 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, child-on-child 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.
- 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.

1.3 The Governing Body will:

The governor who oversees online safety is Parkash Krishan.

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

- The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding leads (DSL/DDSL) or online safety lead.
- The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (See Appendix)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

1.4. The Designated Safeguarding Lead (DSL) Azizan Kabil and Deputy Designated Safeguarding Leads (DDSL) Sarah Andrews, Annette Smith and Jenny Hawkins:

The DSL/DDSLs take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix Logging a MyConcern) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the headteacher and/or governing body
- Provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- 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.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Oversee records for online safety concerns, as well as actions taken, as part of West Park's safeguarding recording systems.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.

1.5. The ICT Team Wolverhampton City Council will:

- 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. Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensure that the 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 the filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.
- Conduct a full security check and monitoring the school's ICT systems on a monthly basis
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure that any online safety incidents are reported to the DSLs.

1.6. Staff and Volunteers are responsible for:

- Maintaining an understanding of this policy, including acceptable use policies and procedures
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (See Appendix) and ensuring that pupils follow the school's terms on acceptable use (See Appendix)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by completing a ticket to Wolverhampton Council (ICT Team) and emailing the headteacher and where relevant logging on MyConcern.

- Working with the DSL /DDSLs to ensure that any online safety incidents are logged on MyConcerns and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- 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.
- Read online safety updates and current research and take personal responsibility for professional development in this area.

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see appendix).

1.7. Parents and Carers are responsible for:

- Reading the acceptable use of technology policies and encouraging their children to adhere to them.
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendix).
- Supporting our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Being role models for safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seeking 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.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

1.8. Pupils (at a level appropriate to their age) are responsible for:

- 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 (see appendix) 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.

Educating Pupils about Online Safety

2.1. National Curriculum

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS1)** , pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS2)** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

2.2. **Educating Pupils**

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.
- 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 using 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.

- involve 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
- 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.

2.3 Educating Vulnerable Pupils

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 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.

2.4 Educating Parents/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:

- Parent/carer workshops
- Newsletters
- The school website and social media channels
- Parents' evenings
- Signpost parents and carers to read the online safety policy.
- Require parents to read our acceptable use policies and discuss the implications with their children.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

2.5 Staff Training

West Park 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
  - Ongoing as part of staff meetings
  - Staff training covers the potential risks posed to learners 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.

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.

Cyber-bullying

3.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of a person or group by another person or group, where the relationship involves an imbalance of power.

3.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

3.3 Confiscating and searching electronic devices

The headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils,
- is evidence in relation to an offence

Before a search, if the headteacher is satisfied that they have reasonable grounds for suspecting any of the above, they will:

- make an assessment of how urgent the search is
- consider the risk to other pupils and staff
- If the search is not urgent, the headteacher will contact parents prior
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- always seek the pupil’s co-operation

The headteacher may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the headteacher should reasonably suspect that the device has, or could be used to:

- cause harm
- undermine the safe environment of the school
- disrupt teaching
- commit an offence

If inappropriate material is found on the device, the headteacher will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE’s latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE’s latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the school complaints procedure.

3.4 Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

West Park recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

West Park will treat any use of AI to bully pupils in line with our behaviour policy.

Safe Use of Technology

4.1. 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 cameras or video cameras.
- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- 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.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- 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 and 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.

4.2 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 (see appendix) before being given access to our computer system, IT resources or the internet.

4.3 Filtering and monitoring

- 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.

4.4 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** which 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.
- 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 (Online Safety Lead) 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.

4.5 Appropriate monitoring

- West Park Primary School uses using **Senso** that 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.

4.6 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 awaiting update from Chris Watabiki

4.7 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 e.g. memory sticks/external storage devices.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools e.g. 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.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

4.8 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 (Online Safety Lead) 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.

4.9 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
- 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.

4.10 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
- 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 is 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 must 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.

4.11 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 records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts will be blocked on site.

4.12 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. Senior leaders use the following signature to remind staff of appropriate work life balance: *This email has been sent at a date and time convenient to me. Please do not feel obliged to respond out of hours.*

4.13 Learner email

- Learners will use a school provided Microsoft account for educational purposes. 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.

4.14 Online 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/Seesaw 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.
- Leaders and staff will regularly monitor the use of Teams/Seesaw 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.

4.15. 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.
- Seesaw is used to record children's learning portfolios and home learning.
- TT Rockstars, SPaG.com, PE Passport are online applications that store children's assessment information.
- The Headteacher or Online Safety Lead 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:
  - 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.

4.16. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters
- All hard drives are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way that would violate the school's terms of acceptable use (see appendix).
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from OSL or ICT Team (Wolverhampton City Council).

Reporting an Online Safety Concern

- All adults must report behaviour and safeguarding issues related to online safety on MyConcerns, including breaches of filtering, child on child 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.

5.1 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 child on child 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.
- The DSL/DDSL will use the online safety concern flowchart to ensure they follow the correct action when an online safety concern is reported in school (see appendix).

5.2 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.

5.3 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.

Social Media

6.1 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 are given access on school devices to Twitter to allow updating of the school's social media channel @westparkpri
  - 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.

- 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.
- 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.
- Members of staff are must 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.

6.2 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.
- 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.

6.3 Official use of social media

- West Park Primary School official social media channels are:
  - *Twitter: @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.
- 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.

Mobile Devices

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.
- 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 classrooms.
- 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.
- 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.
- 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.

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.

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 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 must 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.

Appendix 1

Responding to an Online Safety Concern Flowchart

Key Local Contacts

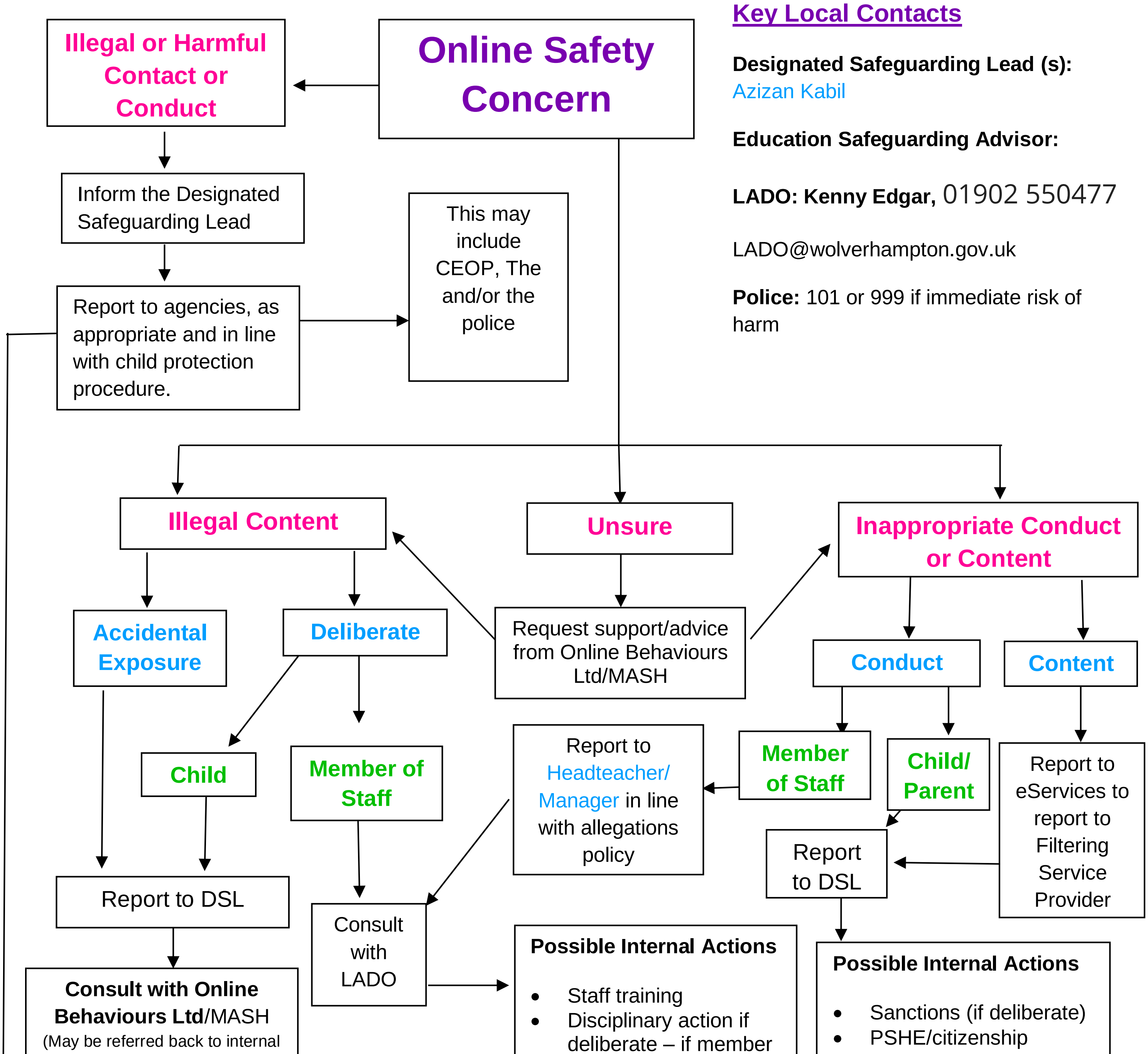
Designated Safeguarding Lead (s): Azizan Kabil

Education Safeguarding Advisor:

LADO: Kenny Edgar, 01902 550477

LADO@wolverhampton.gov.uk

Police: 101 or 999 if immediate risk of harm



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

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

This may include CEOP, The and/or the police

Illegal Content

Unsure

Inappropriate Conduct or Content

Accidental Exposure

Deliberate

Request support/advice from Online Behaviours Ltd/MASH

Conduct

Content

Child

Member of Staff

Report to Headteacher/ Manager in line with allegations policy

Member of Staff

Child/ Parent

Report to eServices to report to Filtering Service Provider

Report to DSL

Consult with LADO

Report to DSL

Consult with Online Behaviours Ltd/MASH

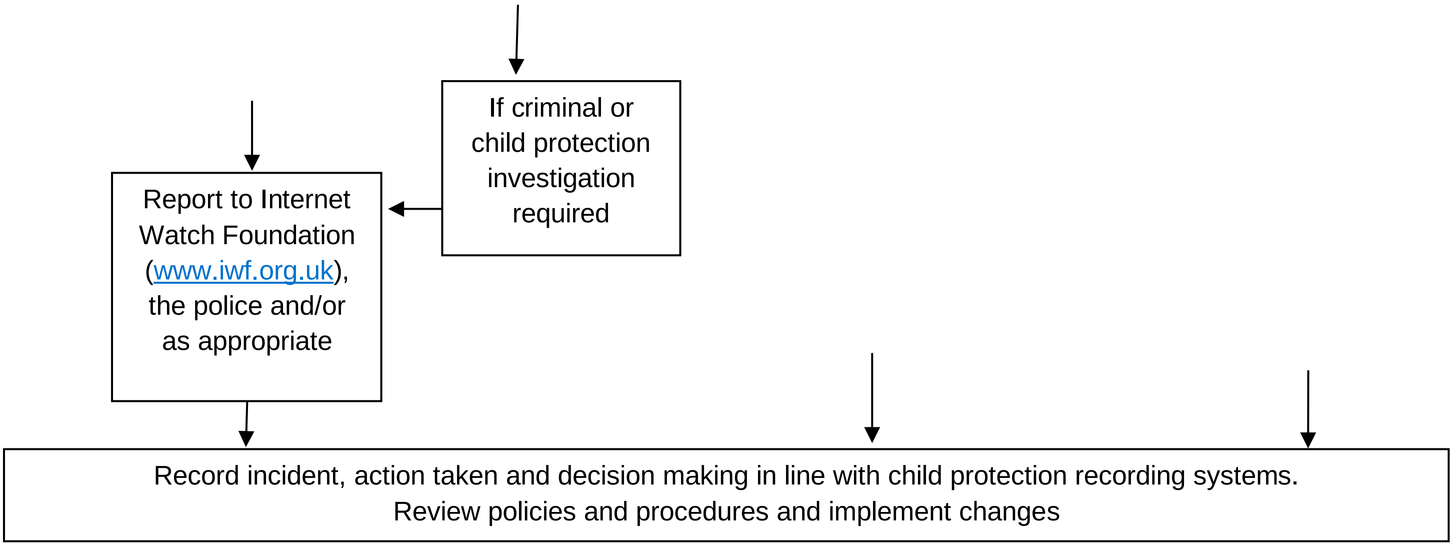
(May be referred back to internal

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship



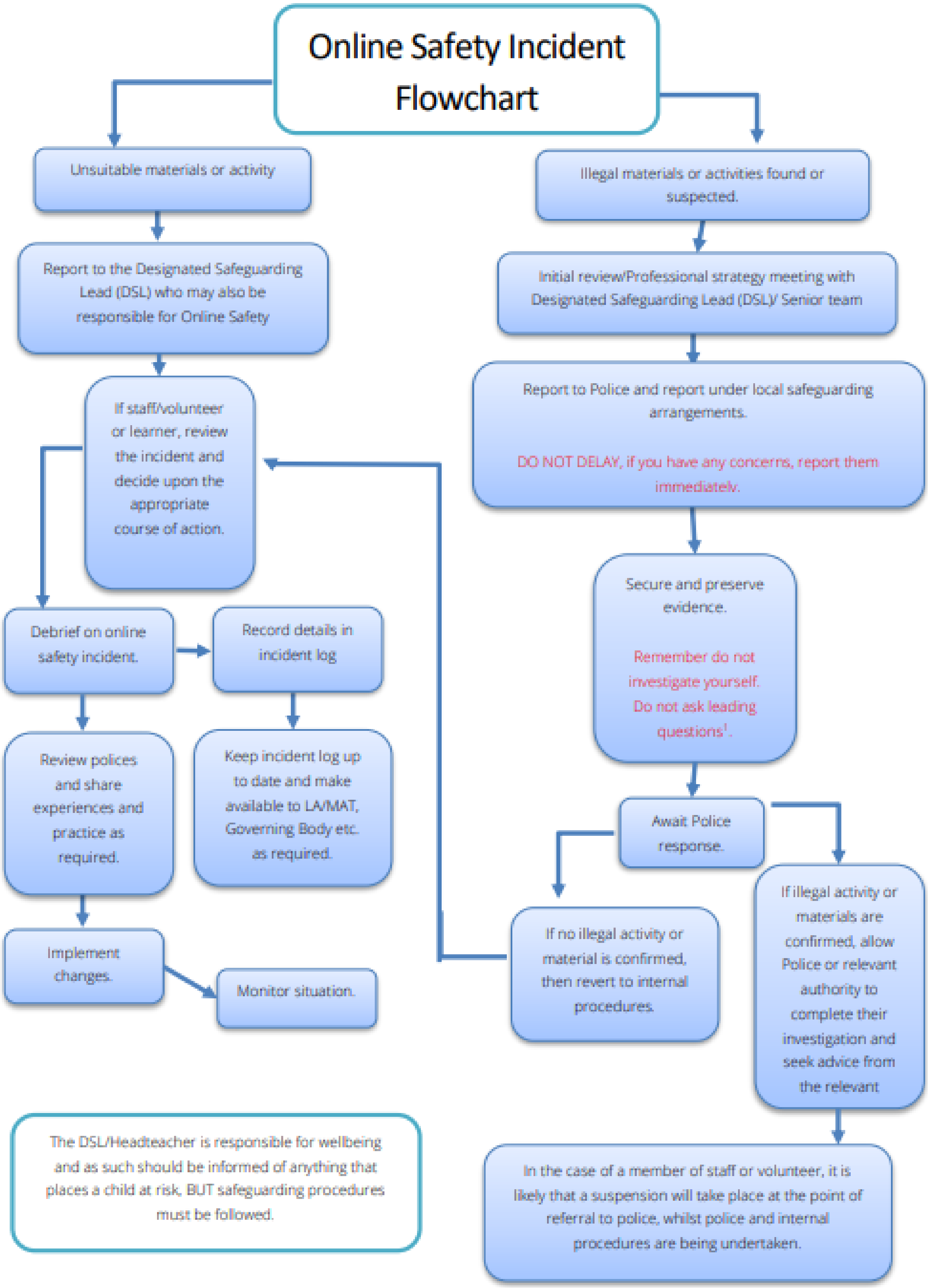
If criminal or child protection investigation required

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

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

Appendix 2

Online Safety Incident Flowchart



Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes.

Monitor situation.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response.

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

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/Sarah Andrews.
3. 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.**
4. 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.
5. 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.
6. 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. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
7. 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.
8. 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.

9. I agree to adhere to all provisions of the school Data Protection Policy 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/Sarah Andrews, if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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, up skirting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy 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.

Name: ________________________________ Signature: ______________________________

Role: ____

Date: ____

West Park Primary

Respect-Aspiration-Resilience-Integrity

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

Acceptable Use Policy (AUP) for KS1 PUPILS

Respect-Aspiration-Resilience-Integrity

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:

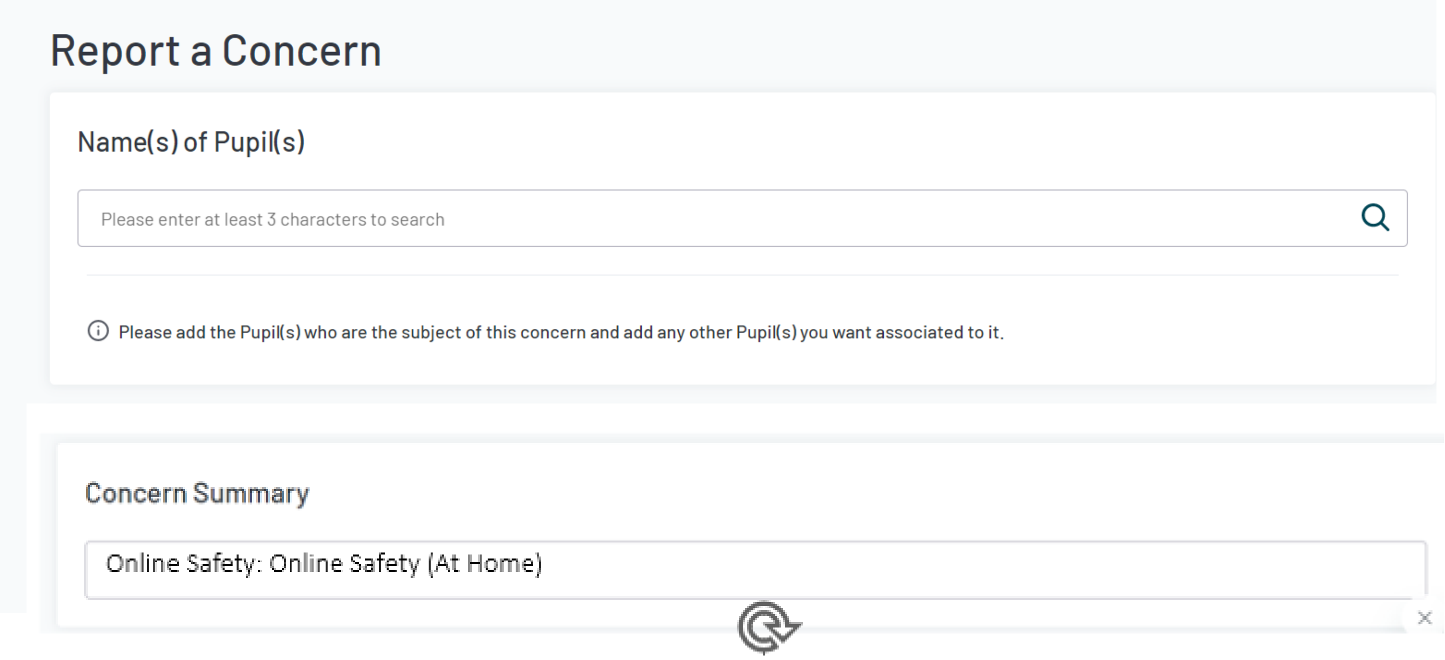
____ **at school**

____ **at home**

For parents/carers

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

Reporting a MyConcern



Report a Concern

Name(s) of Pupil(s)

Please enter at least 3 characters to search

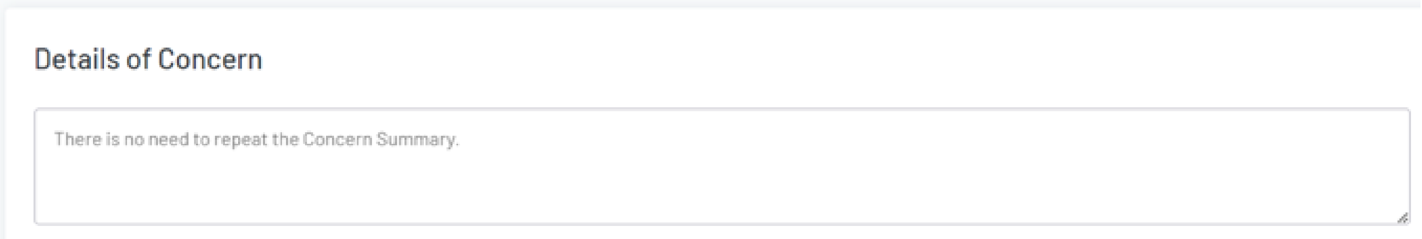
ⓘ Please add the Pupil(s) who are the subject of this concern and add any other Pupil(s) you want associated to it.

Concern Summary

Online Safety: Online Safety (At Home)

Categories for Online Safety

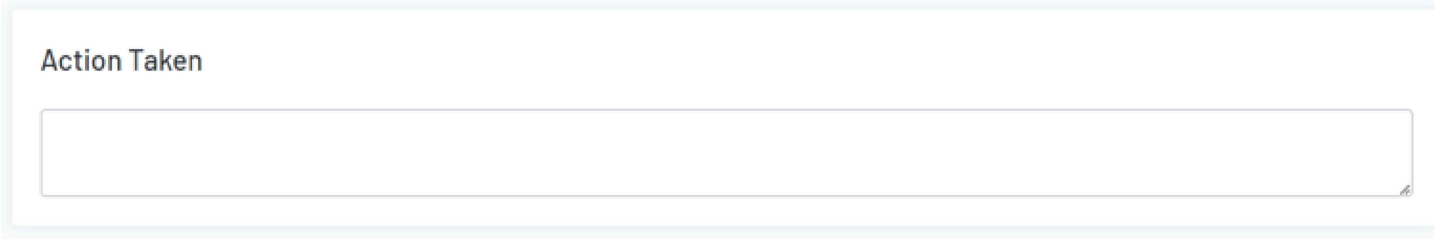
Accessing Age-Inappropriate Material
Bullying (online)
Online Safety (In School)
Online Safety (At Home)
Indecent/Illegal Images
Online Abuse
Online Learning



Details of Concern

There is no need to repeat the Concern Summary.

Safeguarding and Online Safety: Factual Information
Anything you record – may be shared with professionals or family



Action Taken

Professional Curiosity
You must action safeguarding.
Particularly neglect – Remind parents, Phone call/Text Message sent, conversation with parents. You do not need to wait to be instructed by DSL/DDSL to ask questions.
If unsure - always ask!