Green Park Community Primary School
Online Safety Policy 2024 – 2025

Key Details

Designated Safeguarding Lead: Richard Hawkins (Head Teacher)

Named Governor with lead responsibility: Nigel Collins (Chairperson)

Date written: September 2024

Date agreed and ratified by Governing Body: September 2024

Date of next review: September 2025

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

Green Park Community Primary School: Online Safety Policy

1. Policy aims

- This online safety policy has been written by Green Park Community Primary School hereby referred to as 'Green Park'), involving staff, learners and parents/carers, building on the Kent County Council's LADO and Education Safeguarding Advisory Service policy templates, with specialist advice and input as required.
- It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSIE), Early Years and Foundation Stage (EYFS), 'Working Together to Safeguard Children' (WTSC), the DfE non-statutory guidance 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school', 'Mobile Phones in Schools' and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

- The purpose of Green Park's online safety policy is to
  - safeguard and promote the welfare of all members of our 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.

- At Green Park, we recognise that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk.
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
  - **Commerce:** being exposed to gambling, inappropriate advertising, phishing and financial scams

2. Policy scope

- Green Park 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.
- Green Park 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.
- Green Park 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 the Staff Code of Conduct
    - Behaviour policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security
    - Cameras and image use policy
    - Mobile phone and social media policies

3. Monitoring and review

- Technology evolves and changes rapidly; as such Green Park 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 Designated Safeguarding Lead (DSL) (Richard Hawkins - Headteacher) is recognised as holding overall lead responsibility for online safety.

- Green Park recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of 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 (Cantium) 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) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as the Computing Lead, Pastoral team, 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 Headteacher/Senior Leadership Team (SLT) and Governing Body.
- Work with the Computing Lead (in conjunction with the SLT to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

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

- 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, Headteacher and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the Headteacher and SLT 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 Computing Lead, Headteacher and SLT.
- 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.
- 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 learning 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 approach is developed in line with the UK Council for Internet Safety (UKCIS) ‘Education for a Connected World Framework’ and DfE ‘Teaching online safety in school’ guidance.

  - ensuring online safety is addressed in 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.
  - 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.
  - rewarding positive use of technology.

- Green Park 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 with internet access.
  - 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.

- Green Park 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.
  - 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

- Green Park 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.
- Green Park will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at Green Park 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 and acceptable use policies 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.
    - 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 provide 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

- Green Park 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 may include but is not limited to: Safer Internet Day activities, assemblies and visiting speakers.

  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus and on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, within our Home-School Agreement.
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Green Park 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

- Green Park 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
  - Learning platform/intranet
  - 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.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- The setting will use appropriate search tools as identified following an informed risk assessment.
- 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 record of users who are granted access to our devices and systems.
- 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

- Green Park governors, staff and IT management have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The IT management provider will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- Staff 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

- Green Park's education broadband connectivity is provided through Medway Grid for Learning (MGfL).

- Green Park uses Netsweeper Filtering System.
  - Netsweeper 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.
  - Netsweeper is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
  - Netsweeper integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with MGfL and Netsweeper 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 or turn over device and report the concern immediately to a member of technical staff, report the URL of the site to MGfL/Netsweeper.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- 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:
  - Physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or 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 in line with our Safeguarding policies.

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 on the school website (www.greenparkcps.co.uk)

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 sensitive 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 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.
    - Checking files held on our network, as required and when deemed necessary by DSL/SLT.
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all users (where age and ability appropriate).
    - 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.
- We require all users to
    - use strong passwords for access into our system.
    - change their passwords as prompted by the system.
    - 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.
- 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.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the Cameras and Image Use, Data Security, Acceptable Use policies, Code of Conduct, Social Media and Use of Personal Devices and Mobile Phones policies.

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.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting 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 Richard Hawkins (DSL/Headteacher) 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.
- We will have a dedicated system (MyConcerns) for reporting wellbeing and pastoral issues.

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 business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- Learners may use a provided email account for educational purposes.
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses will be used for communication outside of the setting.

7.9 Educational use of videoconferencing and/or webcams

- Green Park recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.

  - ○ Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
  - ○ Videoconferencing contact details will not be posted publicly.
  - ○ Videoconferencing equipment will not be taken off the premises without prior permission from the DSL/Headteacher.
  - ○ Staff will ensure that external videoconferencing opportunities and tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
  - ○ Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

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

8. Social Media

8.1 Expectations

Green Park Community Primary School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in may ways, the same standards of behaviour are expected online as they are offline.

- The expectations' regarding safe and responsible use of social media applies to all members of Green Park 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 messengers.
- All members of Green Park community are expected to engage in social media in a positive and responsible manner.
    - All members of Green Park 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.
    - The use of social media during school hours for personal use is not permitted for learners.
    - The use of social media during school hours for sharing of information to the school social media platforms is permitted for staff.
    - 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 Green Park community on social media, will be reported to the DSL (Richard Hawkins) and be managed in accordance with our Anti-bullying Policy, Whistleblowing/Allegations Against Staff Policy, Behaviour Policy and Child Protection Policy.

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 and Acceptable Use of Technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of their induction training. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as and when they become available.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously and dealt with in line with our Child Protection Policy and Whistleblowing/Allegations Against Staff 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 Green Park on their personal social networking accounts; this is to prevent information being linked with the school 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 pupils and parents/carers

- Staff will not use personal social media accounts to contact pupils, nor should any contact be accepted.
- Staff may use their personal social media accounts to access the official school social media platforms and to communicate to parents/carers. This is at the discretion of each member of staff and they are advised to only use the publicly visible means of communication (not to use private messages).
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as ‘friends’ on any personal social media sites, applications or profiles.
- 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 parents received on personal social media accounts should be saved and discussed with a member of SLT or the Headteacher as appropriate.

8.3 Pupils use of social media

- The use of social media during school hours for personal use is not permitted for pupils.
- Many online behaviour incidents amongst children take place on social media outside of school hours and outside of the school premises. Parents/carers are responsible for monitoring this online behaviour; however where these incidents may cause harm to another pupil, impact the safety of the school or damages the reputation of the school, action will be taken in line with our Child Protection Policy.
- Pupils will be empowered to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop the resilience to manage and respond to online risks through an embedded and progressive education approach via age appropriate sites and resources. Further information is contained in the Relationships and Sex Education Policy and Computing Policy.
- 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 pupils use of social media will be dealt with in accordance with existing policies, including the Anti-bullying Policy and Behaviour Policy.
- The DSL (Richard Hawkins) will respond to social media concerns involving safeguarding or child protection risks in line with the Child Protection and Safeguarding Policy.
- Sanctions and pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with the Child Protection Policy.
    - Civil or legal action may be taken if necessary.
- Concerns regarding pupils use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Pupils will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others 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

- Green Park official social media channels are:
    - Twitter - @greenparkschool
    - Facebook - Official Green Park School (staff run page), Green Park Primary School: The Foundation Stage, Green Park Primary School: Year 1, Green Park Community

Primary School: Years 2 and 3, Green Park Community Primary School: Years 4 and 5, Green Park Community Primary School - Year 6.

- The official use of social media sites by Green Park 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
    - The Headteacher, Computing Lead and Leaders of Learning 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.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; 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

- Members of staff who follow and/or like our official social media channels will be advised to set their accounts to private and refuse friend requests/private messages to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure appropriate consent has been given before sharing images on the official social media channel.

  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any private/direct messaging with current or past learners or parents/carers.
  - Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

8.5 Policy Monitoring and Review

- Technology evolves and changes rapidly. This policy will be reviewed at least annually. The policy will be revised following any national or local updates, concerns and changed to our technical infrastructure.
- Regular monitoring of internet usage takes place via our provided devices and systems and we evaluate online safety procedures to ensure that this policy is consistently applied.
  - Any issues identified will be incorporated into our action planning.
- All members of the school will be made aware of how the school will monitor policy compliance.

8.6 Responding to Policy Breaches

- All members of the school will be informed of the need to report policy breaches or concerns to the DSL (Richard Hawkins).
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and pupils to work in partnership with us to resolve issues.
- All members of the school will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents/carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL/Headteacher (Richard Hawkins) or a deputy will seek advice from The Education People's Education Safeguarding Service or other agencies in accordance with the Child Protection Policy.

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

- Green Park Community Primary School recognises that personal communication through mobile technologies is part of everyday life for many pupils, staff and parents/carers.

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 and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

    - All members of the school 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 the school 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 toilets and are discouraged from use in public areas during school hours.
- The sending of abusive or inappropriate messages or content, including via mobile phones or personal smart 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 Green Park 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 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.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and Headteacher.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and will only use work-provided equipment for this purpose.
    - To work directly with learners and will only use work-provided equipment during lessons/educational activities.
- Where remote/online learning activities take place, staff, pupils and parents/carers will follow the guidance set out in the Acceptable Use of Technology Policy.

- 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 Pupils use of Mobile and Smart Technology

Behaviour in School: Advice for Headteachers and School Staff 2022 states:

"Headteachers should decide if mobile phones can be used in the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduced complexity and risks, including distraction, disruption, bullying and abuse, and can be detrimental to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.

If Headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils staff and parents/carers throughout the school year. Headteachers should ensure it is consistently and fairly applied."

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology and will be made aware of behaviour expectations and consequences for policy breaches.
    - Mobile phones and personal devices are not permitted on site for all pupils.
    - Smart devices such as Fitbits and health trackers will be permitted at the discretion of the school, and all alerts and notifications should be silenced during the school day.
- Safe and appropriate use of mobile and smart technology will be taught to pupils as apart of an embedded and progressive safeguarding education approach using age-approriate sites and resources. Further information is contained in the Child Protection Policy, the RSE Policy and the Computing Policy.
- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone via the reception desk.
- If a pupil requires access to a personal device in exceptional circumstances, for example medical assistance or monitoring, this will be discussed with the Headteacher prior to use being permitted.
    - This will be documented and recorded by the school
    - Any specific agreements concerning the use (and misuse) of such devices will be provided in writing to the pupil and parents/carers and must be agreed to before use is permitted.
    - Exemptions may be withdrawn by the Headteacher at any time.
- Where pupils use a mobile phone or smart device for remote/online learning, this will be subject to the Remote/Online Learning Acceptable Use of Technology Policy.

9.3.1 Screening, Searching and Confiscation of Electronic Devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding pupils' use of mobile technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.
- Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
- Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers at the end of the day.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a child/pupils/student'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
- If deemed to be necessary and appropriate, searches of mobile phones or personal devices may be carried out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that they understand:

    - Mobile phones and personal devices are only permitted within specific areas or are only permitted for specific purposes, for example as part of a multi-agency working arrangement.
- Appropriate signage and information is provided to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including but not limited to Child Protection and Image Use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL/Headteacher (Richard Hawkins) or deputy of any breaches of our policy.

9.5 Officially provided mobile phones and devices

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

9.6 Policy Monitoring and Review

- Technology evolves and changes rapidly. This policy will be reviewed at least annually. The policy will be revised following any national or local updates, concerns and changed to our technical infrastructure.
- Regular monitoring of internet usage takes place via our provided devices and systems and we evaluate online safety procedures to ensure that this policy is consistently applied.
    - Any issues identified will be incorporated into our action planning.
- All members of the school will be made aware of how the school will monitor policy compliance.

9.7 Responding to Policy Breaches

- All members of the school will be informed of the need to report policy breaches or concerns to the DSL (Richard Hawkins).
- Where pupils breach this policy:
    - Appropriate sanctions and pastoral/welfare support will be implemented and offered in line with the Behaviour Policy and Child Protection Policy.
    - Concerns will be shared with parents/carers where appropriate.
    - We will respond in line with the Child Protection Policy if there is a concern the child is at risk of harm.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and pupils to work in partnership with us to resolve issues.

- All members of the school will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents/carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL/Headteacher (Richard Hawkins) or a deputy will seek advice from The Education People's Education Safeguarding Service or other agencies in accordance with the Child Protection 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/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.
- Green Park 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 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 agreement, 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 Online sexual violence and sexual harassment between children

- Our Headteacher, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- Green Park 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.
    - 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.
- Green Park 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.
- Green Park recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Green Park 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")

- Green Park 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: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- Green Park 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.
- 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 and KSCMP 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 and KSCMP 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 and KSCMP 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)

- Green Park 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.
- Green Park 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.
- 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 KSCMP 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)

- Green Park 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 KSCMP 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 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Green Park.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online hate

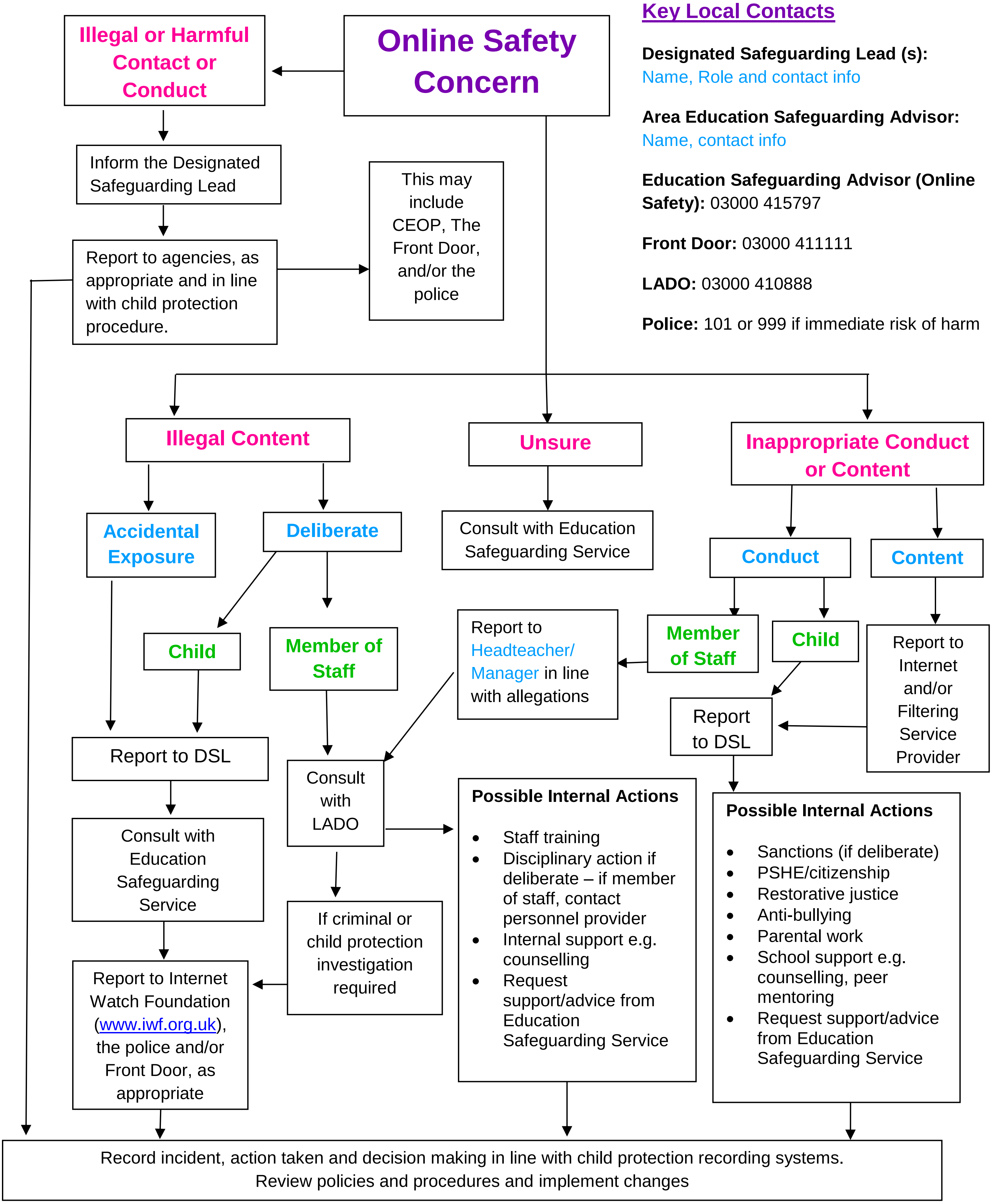
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Green Park and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online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

September 2019

Responding to an Online Safety Concern Flowchart



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 Front Door, and/or the police

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

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

Consult with LADO

If criminal or child protection investigation required

Unsure

Consult with Education Safeguarding Service

Report to Headteacher/ Manager in line with allegations

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

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

Key Local Contacts

Designated Safeguarding Lead (s):
Name, Role and contact info

Area Education Safeguarding Advisor:
Name, contact info

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm

Useful Links

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 of Technology Policy (AUP)

Learner Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I always tell a member of staff if something online makes me feel unhappy or worried
- I can visit sites such as www.thinkuknow.co.uk to learn more about keeping safe online
- I know that if I do not follow the rules:
    - I may lose access to Technology devices within school
    - My parents/carers will be notified
- I have read and talked about these rules with my parents/carers

Key Stage 2 (7-11)

Safe

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

Learning

- I ask my teacher before using the internet
- I only use websites and search engines that are approved by Green Park Community Primary School and the Netsweeper Filtering system
- I only use school devices for school work, unless I have permission to do otherwise
- If I need to learn online from home, I will follow the school’s Remote/Online Learning AUP

Trust

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

Responsible

- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if teacher has allowed me to

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored to keep me safe
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I know that if I do not follow the school rules then:
    - I may lose access to Technology devices within school
    - My parents/carers will be notified

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher
- I know it is not my fault if I see, or someone sends me, something bad online. I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will turn off the screen/turn over the device and tell an adult straight away

Learners with SEND functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I don't like online, I tell a grown up
- I know that if I do not follow the school rules then:
    - I may lose access to Technology devices within school
    - My parents/carers will be notified

Learners with SEND functioning at Levels P7-L1

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- On the internet I don't tell strangers my name
- I know that if I do not follow the school rules then:
    - I may lose access to Technology devices within school
    - My parents/carers will be notified

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I don't open messages or emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see anything that I don't like online, I will tell a grown up

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then:

  - I may lose access to Technology devices within school
  - My parents/carers will be notified

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

Accepting

- I don't open messages from strangers
- I check web links to make sure they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see anything online that I don't like, I will tell a teacher

Green Park Community Primary School Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP) and Remote/Online Learning AUP.

I agree to follow the AUP when:

1. I use school systems and devices, both on and offsite
   Including, but not limited to:
   -Computers (in class and in the Computer Suite)
   -iPads
   -Times Tables Rock Stars and Numbots
   -Lexia
   -School Website
   -Purple Mash
   -Accelerated Reader
   -White Rose 1-Minute Maths
   -Pixl

2. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school or accessing school email or website.

Name……………………………………………….

Class………………………. Date…………………….

Green Park Community Primary School Learner Acceptable Use of Technology Policy: Parental Acknowledgment

1. I have read and discussed Green Park Community Primary School's Acceptable Use of Technology Policy (AUP) and Online/Remote Learning AUP. I understand that these documents will help keep my child safe online.

2. I understand that the AUP applies to the use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behavioural concerns. **This may include, but is not limited to, if online behaviour poses a threat or causes harm to another pupil, could have an impact on school safety or damage the reputation of the school**

3. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reasons to keep both my child, and others, safe.

4. I am aware that the Mobile and Smart Technology Policy states that my child cannot bring, or use, any personal mobile devices or smart technology within school.

5. I understand that my child may need a safe and appropriate place to access remote/online learning and I will ensure my child's access to remote/online learning will be appropriately supervised.

6. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and school devices. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online.

7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school or wider community or damage the reputation of the school.

8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

11. I understand my role and responsibility in supporting the school's online safety approaches and keeping my child safe online. I will use appropriate parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home.

Child's Name…………………………………………........ Class…………………………

Parents Name………………………………………….......

Parents Signature…………………………. Date……………

Staff Acceptable Use of Technology Policy

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

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

Policy Scope

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

2. I understand that Green Park Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's Child Protection Policy, Online Safety Policy and Staff Code of Conduct.

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

Use of School Devices and Systems

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

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed outside of teaching hours and when not in the presence of learners.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

- I will use a ‘strong’ password to access school systems.
- I will protect the devices in my care from unapproved access or theft.

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

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

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

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.

11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school network or Microsoft OneDrive (school account) to store any work documents and files in a password protected environment.

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

13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Computing Lead or IT system manager as soon as possible.

16. If I have lost any school related documents or files, I will report this to the Headteacher (Richard Hawkins) and school Data Protection Officer (Belinda Daniels) as soon as possible.

Classroom Practice

17. I am aware of safe technology use in the classroom, safe remote learning and other working spaces, including appropriate supervision of learners, as outlined in the school's Child Protection Policy and Online Safety Policy.

18. I have read and understood the school's Online Safety Policy and Mobile, Smart Technology and Social Media Policy.

19. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Richard Hawkins) or a deputy (Maria Harrison) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

20. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school's Child Protection Policy and Online Safety Policy.

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

Mobile Devices and Smart Technology

22. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the

Staff Code of Conduct, the Online Safety Policy, the Mobile, Smart Technology and Social Media Policy and the law.

Online Communication, including Use of Social Media

23. I will ensure that my use of communication technology, including the use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Child Protection Policy, Online Safety Policy, Mobile, Smart Technology and Social Media Policy, Staff Code of Conduct and the law.

24. As outlined in the Staff Code of Conduct, Online Safety Policy and Mobile, Smart Technology and Social Media Policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school online, when using communication technology, including the use of social media.
    - I will not discuss, or share, data or information relating to pupils, staff, school business or parents/carers on social media.

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

Policy Concerns

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

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

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

29. I will report and record any concerns about the welfare, safety or behaviour, of pupils or parents/carers online to the DSL (Richard Hawkins) in line with the Child Protection Policy.

30. I will report and record any concerns about the welfare, safety or behaviour, of staff online to the Headteacher (Richard Hawkins) in line with the school's Child Protection Policy and Whistleblowing/Allegations Against Staff Policy.

Policy Compliance and Breaches

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

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

33. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff Code of Conduct.

34. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff Code of Conduct.

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

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

Name of staff member: …………………………………………………………………………

Signed: ……………………………..

Date (DDMMYY)………………………………………………...

Visitor and Volunteer Acceptable Use of Technology Policy

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

Policy Scope

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

2. I understand that Green Park AUP should be read and followed in line with the school staff Code of Conduct.

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

Data and Image Use

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

5. I understand I am not allowed to take images or videos of pupils, unless expressly permitted by the Headteacher (Richard Hawkins) or a member of staff on their behalf.

Classroom Practice

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

7. Where I deliver or support remote/online learning, I will comply with the Remote/Online Learning Policy.

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the pupils in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the Designated Safeguarding Lead (DSL) (Richard Hawkins) in line with the school's Child Protection Policy and Online Safety Policy.

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

Use Mobile Devices and Smart Technology

11. I understand that mobile phones and personal devices are not permitted on my person without expressed consent from the Headteacher (Richard Hawkins) or a member of staff of their behalf.

Online Communication, including Use of Social Media

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

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

Policy Breaches or Concerns

14. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead/Headteacher (Richard Hawkins).

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

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

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

18. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Richard Hawkins) in line with the school online safety/child protection policy.

19. I will report concerns about the welfare, safety or behaviour of staff online to the Headteacher, in line with the allegations against staff policy.

20. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

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

I have read, understood and agreed to comply with the Green Park Community Primary School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ………………………………………………………………………………

Signed: ………………………...

Date (DDMMYY)……………………………………………….....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The school provides Wi-Fi for the school community and allows access for educational purposes.

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

3. The use of technology falls under Green Park Acceptable Use of Technology Policy (AUP), Online Safety Policy, Mobile, Smart Technology and Social Media Policy and Code of Conduct which all pupils/staff/visitors and volunteers must agree to and comply with.

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

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

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

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

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

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

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

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

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Richard Hawkins) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead/Headteacher (Richard Hawkins).

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

I have read, understood and agreed to comply with the Green Park Community Primary School Wi-Fi acceptable Use Policy.

Name …………………………………………………………………………………...

Signed: ………………………...Date (DDMMYY)………………

Remote/Online Learning Acceptable Use of Technology Policy

Green Park Community Primary School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of the school community when taking part in remote/online learning, for example following any full or partial school closures.

Leadership oversight and approval

1. Remote/online learning will only take place using the following approved platforms:
   Zoom
   Microsoft Teams
   Via the school website and associated Facebook pages.
   - These platforms have been assessed and approved by the Headteacher (Richard Hawkins) and the Senior Leadership Team (SLT).

2. Staff will only use school managed or specific, approved professional accounts with pupils and parents/carers.
   - Use of any personal accounts to communicate with pupils and parents/carers is not permitted.
     - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL) (Richard Hawkins).

3. Online contact with pupils and parents/carers will only take place outside of the usual school day when deemed appropriate by the Headteacher (Richard Hawkins), SLT or members of teaching staff.

4. All remote/online lessons will be formally timetabled and the Headteacher (Richard Hawkins), a member of SLT or another member of staff, as approved by SLT, is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from Headteacher (Richard Hawkins) and SLT.

Data Protection and Security

6. Any personal data used by staff and captured by these platforms when delivering remote learning will be processed and stored with appropriate consent and in accordance with our Data Protection Policy.

7. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the Staff Code of Conduct.

8. All participants will be made aware that these platforms records activity.

9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

10. Only members of Green Park Community Primary School will be given access to these platforms.

Session management

11. Staff will record the length, time, date, and attendance of any sessions held.

12. Appropriate privacy and safety settings will be used to manage access and interactions.

13. A pre-agreed email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Pupils and parents/carers should not forward or share access links.
    - If pupils or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

14. Alternative approaches or access will be provided to those who do not have access.

Behaviour expectations

15. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

16. All participants are expected to behave in line with existing school policies and expectations. This includes
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Other attendees cannot record events for their own use under any circumstances.

17. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

18. When sharing pre-recorded videos or taking part in live lessons, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

19. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

20. Participants are encouraged to report concerns during remote or live-streamed sessions to the member of staff running the session immediately.

21. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the Headteacher/DSL (Richard Hawkins).

22. Inappropriate online behaviour will be responded to in line with existing policies, including Online Safety Policy, Acceptable Use of Technology Policy (AUP), Whistleblowing/Allegations Against Staff Policy, Anti-bullying Policy and Behaviour Policy.

23. Sanctions for deliberate misuse may include restricting/removing use or contacting police if a criminal offence has been committed.

24. Any safeguarding concerns will be reported to Richard Hawkins, Designated Safeguarding Lead, in line with our Child Protection Policy and Online Safety Policy.

I have read and understood the Green Park Community Primary School Staff Remote/Online Learning Acceptable Use Policy

Staff Member Name: ……………………………………………………………………………………………

Date………………………………………………………………………………………………………

September 2019

Green Park Community Primary School Pupil Remote/Online Learning AUP

1. I understand that:
   - these expectations are in place to help keep me safe when I am learning at home using Zoom and Microsoft Teams.
   - I should read and talk about these rules with my parents/carers.
   - remote/online learning will only take place using these platforms and during usual school times.
   - my use of these platforms is monitored to help keep me safe.

2. Only members of Green Park Community Primary School can access these sessions.
   - I will only use my school provided email accounts or login to access remote learning.
   - I will use privacy settings as agreed with my teacher/set up the school.
   - I will not share my login/password with others.
   - I will not share any access links to remote learning sessions with others.

3. When taking part in remote/online learning I will behave as I would in the classroom. This includes:
   - Using appropriate language.
   - Not taking or recording images/content without agreement from the teacher and/or those featured.

4. When taking part in live sessions I will:
   - mute my video and microphone as requested by the adult leading the session.
   - wear appropriate clothing and be in a suitable location.
   - ensure backgrounds of videos are neutral and personal information/content is not visible.
   - use appropriate alternative backgrounds.
   - attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
   - attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote/online learning, I will:
   - Tell the member of staff running the session immediately, or speak to a parent/carer.

6. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously. This could include:
   - restricting/removing access, informing parents/carers and contacting police if a criminal offence has been committed.

I have read and understood the Green Park Community Primary School Pupil Remote/Online Learning Acceptable Use Policy

Name……………………………………………….

Class………………………………...………… Date………………………………………….……….