Lydden and River Primary Schools Federation

Online Safety Policy

Key Details

Designated Safeguarding Lead (s): Mrs V Alliston- River Primary School, Head of School. Mrs C Lintott – Lydden Primary School, Head of School

Named Governor with lead responsibility: Dr K Grilli

Date written/updated: September 2023

Date agreed and ratified by Governing Body: October 2023

Date of next review: September 2024

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.

Lydden and River Primary Schools Federation

Online Safety Policy

1. Policy Aims and Scope

- This policy has been written by Lydden and River Primary Schools Federation, involving staff, learners and parents/carers, building on The Education People policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage, 'Working Together to Safeguard Children' and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all learners and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate learners and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
- Lydden and River Primary Schools Federation understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
    - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- Lydden and River Primary Schools Federation recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online.
- This policy applies to learners, parents/carers and 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 school (collectively referred to as "staff" in this policy).
- Lydden and River Primary Schools Federation identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.
- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Staff Code of Conduct
    - Behaviour policy
    - Safeguarding and Child protection policy
    - Confidentiality policy

- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection (GDPR policy)
- Image use policy
- Mobile and smart technology
- Social media

2. Responding to Emerging Risks

- Lydden and River Primary Schools Federation recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our learners face.
  - 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 is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate. In line with KCSIE 2023 and our updated Safeguarding and Child Protection policy.
  - 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, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

- Lydden and River Primary Schools Federation will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head of Schools/Executive 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 will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Mrs V Alliston – Head of School, River Primary School and Mrs C Lintott, Lydden Primary School are recognised as holding overall lead responsibility for online safety, however Lydden and River Primary Schools Federation 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 school culture that incorporates online safety throughout.

- 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 which address the acceptable use of technology, child on child abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- 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 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 school curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Leads (DSL) will:

- Act as a named point of contact on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety as appropriate.
- Ensure referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools 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, including 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 schools 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 senior leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding.

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

- Contribute to the development of our online safety policies.

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

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

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

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

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

4.6 It is the responsibility of parents and carers to:

- Read our Acceptable Use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies if they or their child encounter online issues.

- Contribute to the development of our online safety policies.
- Use our systems, such as 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

- Lydden and River Primary Schools Federation will establish and embed a whole school culture and will empower our learners to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- We 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 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 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. 'Using External Visitors to Support Online Safety Education: Guidance for Educational Schools'.
    - providing online safety education as part of the transition programme across the key stages and when moving between establishments.
    - rewarding positive use of technology.
- Lydden and River Primary Schools Federation will support learners to understand and follow our Acceptable Use policies in a way which suits their age and ability by:
    - sharing our acceptable use policies with them in accessible and appropriate ways.
    - 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.
- Lydden and River Primary Schools Federation 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.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- 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.
- 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

- Lydden and River Primary Schools Federation recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs or disabilities, who may be more susceptible or may have less support in staying safe online.
- Lydden and River Primary Schools Federation will ensure that differentiated and appropriate online safety education, access and support is provided to all learners in our specialist resource provision as a follow up to their mainstream lessons. Children in mainstream classes with individual needs benefit from differentiated support within these lessons to ensure full understanding appropriate to their stage of development.
- Staff at Lydden and River Primary Schools Federation will seek input from specialist staff as appropriate, including the DSL, SENCO to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will:
  - provide and discuss the online safety policy and procedures, including our acceptable use policy, with all members of staff as part of induction.
  - provide up-to-date and appropriate training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be achieved as part of existing annual safeguarding and child protection training/updates and within a series of staff development sessions.
  - ensure staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
  - build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
  - ensure staff are 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.
  - ensure staff are 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

- Lydden and River Primary Schools Federation recognises that parents and carers have an essential role to play in enabling our learners to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
  - providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training, website support and highlighting online safety at other events.
  - 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 of technology policies and discuss the implications with their children.

6. Safer Use of Technology

6.1 Classroom use

- Lydden and River Primary Schools Federation 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 platforms, remote learning platform/tools and intranet
  - Email
  - Digital cameras, with recording facilities.
- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place. This includes:
  - School filtering systems - Smoothwall
  - Ipad/Laptop management control and monitoring (Only IT contractor can download and install Apps).
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use appropriate search tools as identified following an informed risk assessment. **SWGfL Swiggle** is used on laptops.
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. Children are not permitted to access Vimeo or Youtube on these devices unless it is to watch the school's private channel.
- 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. This includes:
    - **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.
        - All access will be supervised.

6.1 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, before being given access to our computer system, IT resources or the internet.
- We will maintain a record of users who are granted access to our devices and systems.

6.2 Filtering and monitoring

Appropriate filtering and monitoring on school/college devices and networks

Please see the Appropriate Filter Provider Response in Appendix 2

- Lydden and River Primary Schools Federation will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.

- When implementing appropriate filtering and monitoring, Lydden and River Primary Schools Federation will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.
    - Pupils will use appropriate search tools (Swiggle), apps (controlled by SLT and IT service provider) and online resources as identified by staff, following an informed risk assessment.
    - Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm:
        - AUPs can be found on each school website under the policies section and for staff in our safeguarding and child protection folder under school policies.

Responsibilities

- Our governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

- Mrs V Alliston (DSL), River and Mrs C Lintott (DSL), Lydden and Mr A Richards, governor, are responsible for ensuring that our school/college has met the DfE Filtering and monitoring standards for schools and colleges.

- Our senior leadership team are responsible for
    - procuring filtering and monitoring systems.
    - documenting decisions on what is blocked or allowed and why.
    - reviewing the effectiveness of our provision.
    - overseeing reports.
    - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
    - ensuring the DSL and IT service providers/staff have sufficient time and support to manage their filtering and monitoring responsibilities.
- The DSL has lead responsibility for overseeing and acting on:
    - any filtering and monitoring reports.
    - any child protection or safeguarding concerns identified.
    - checks to filtering and monitoring system.
- The IT service providers/staff have technical responsibility for:
    - maintaining filtering and monitoring systems.
    - providing filtering and monitoring reports.
    - completing technical actions identified following any concerns or checks to systems.
    - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team and business manager works closely with the DSL and the IT service providers/staff. Decisions have been recorded and informed by an approach which ensures our systems meet our federation specific needs and circumstances, including but not limited to our pupil risk profile and specific technology use.

- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

- Our Federation undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.
- In addition, our Federation IT technician, Miss S Higgins, alongside our DSLs undertake regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the governing body that we are meeting our safeguarding obligations.
    - These checks are achieved by:

River:

✓ S Higgins and V Alliston, DSL or a Deputy DSL on a two weekly basis.
✓ Checks are undertaken in a location where confidentiality can be achieved, during working hours, when pupils/students are not present (in the head of school's office)
✓ Using SWGfL testfiltering.com on a range of machines enables users to test fundamental capabilities of our filtering system and to inform improvement.
✓ Checks are logged/recorded, any technical concerns are flagged to the IT staff/IT service provider and safeguarding concerns are actioned by the DSL etc.in line with this policy.

Lydden

✓ S Higgins and C Linott, DSL or a Deputy DSL on a monthly basis.
✓ Checks are undertaken in a location where confidentiality can be achieved, during working hours, when pupils/students are not present (in the head of school's office)
✓ Checks are logged/recorded, any technical concerns are flagged to the IT staff/IT service provider and safeguarding concerns are actioned by the DSL etc.in line with this policy.
✓ Using SWGfL testfiltering.com on a range of machines enables users to test fundamental capabilities of our filtering system and to inform improvement.

Appropriate filtering

- Lydden and River Primary school's education broadband connectivity is provided through Cantium and Lydden and River Primary school use their Smoothwall Filtering system.
    - Smoothwall is a member of Internet Watch Foundation (IWF) verified July 2023.
    - Smoothwall has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) verified July 2023.
    - Smoothwall is blocking access to illegal content including child sexual abuse material (CSAM).
    - Smoothwall 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.

- We filter internet use on all Federation owned, or provided, internet enabled devices and networks. This is achieved by:
    - At Lydden and River Primary Schools Federation we adhere to the filtering of Smoothwall on all devices. Headteacher has to give approval to Cantium via written response to request access for specific items.

  - There are some exclusions:
  - Teacher logins are allowed access to youtube, BBC domain including children is unblocked.
  - Key Personnel logins are approved to allow social media access (for access to school facebook page).
  - The school uses iPad devices. These devices are controlled by Apple School Management central system, using Miraki under PJA Systems Ltd. Please note this will change when the school moves to a new provider in October 2023.
  - The schools can contact Cantium to identify device name or IP addresses, and where possible, individual users, the time and date of attempted access and the search term or content being blocked.

- Our filtering system is operational, up to date and is applied to all users, all federation owned devices and networks, and all devices using the school broadband connection.

- We work with Cantium/Smoothwall and our IT service providers/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
  - Report the concern immediately to a member of staff
  - Staff will turn off monitor/screen or cover device
  - Staff will then report the URL of the site to IT technician or DSL who will log on Cantium's Servicenow Portal.
  - DSL and IT technician will review the breach.

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and code of conduct policies.

- Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services.

- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or IT technician.

Appropriate monitoring

- We will appropriately monitor internet use on all Federation provided devices and networks. This is achieved by:
  - Physical monitoring (supervision)

- Monitoring internet and web access (reviewing logfile information). This can be achieved through contacting Cantium. Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device.

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation; eg through AUP, Code of Conduct and Volunteer/Visitor AUP (ie on InVentry sign-in screen)

- If a concern is identified via our monitoring approaches:
  - Where the concern relates to pupils, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and Code of Conduct policies.
  - Where the concern relates to staff, it will be reported to the Head of School or Executive Headteacher (or Chair of Governors if the concern relates to the Executive Headteacher), in line with our 'Managing Allegations against Staff' policy.

- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services.

6.3 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 data protection policy which can be accessed at www.river.kent.sch.uk/policies or www.Lydden.kent.sch.uk/policies

6.4 Information security and access management

- We take appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and learners.
- Further information about technical environment safety and security includes:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - 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 leadership staff.
  - The appropriate use of user logins and passwords to access our network and user logins and passwords will be enforced for all users.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

6.5.1 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.

- From year 3 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system.
    - change their passwords regulalry
    - 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.

6.5 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 school 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 school 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.

6.6 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 image use, data protection, acceptable use policies, codes of conduct, social media and use of personal devices and mobile phones policies.

6.7 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.
- School email addresses and other official contact details will not be used to set up personal social media accounts.

- Members of the community will immediately report offensive communication to (Mrs V Alliston – River Primary School, Head of School. Mrs C Lintott – Lydden Primary School, Head of School. Mr N Brinicombe – Executive Headteacher).
- 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 email for reporting wellbeing and pastoral issues. This inbox will be managed by the Designated Lead for Mental Health at River and the pastoral TA at Lydden.

6.8.1 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.
    - are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

6.8.2 Learner email

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

6.8 Educational use of videoconferencing and/or webcams

- Lydden and River Primary Schools Federation recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
- Video conferencing is setup by class teachers in order for the class to interact with a virtual visitor. For example when learning about a synagogue in RE or to interact with live events as a whole class.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Videoconferencing 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.

6.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, generally via the teacher laptop to the whole class.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

6.9.2 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.

6.10 Management of learning platforms

- Lydden and River Primary Schools Federation uses Microsoft Office 365 as its official learning platform and all access and use takes place in accordance with our acceptable use policies.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP. When staff and learners leave the school, their account will be disabled or transferred to their new establishment.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

6.11 Management of applications (apps) used to record progress

- We use Target Tracker to track learners progress and share appropriate information with parents and carers.
- The Heads of school/Executive Headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

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

6.12 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- Lydden and River Primary Schools Federation will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems (Microsoft 365).
  - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL or deputies.
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour policy, code of conduct and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Lydden and River Primary Schools Federation will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

7. Responding to Online Risks and/or Policy Breaches

- 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.
  - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This may include: code of conduct for staff, AUPs for staff, visitors and children, child protection policy, whistleblowing policy, Image Use policy, Mobile and Smart technology policy and Social Media policy.
  - will respect confidentiality and the need to follow the official procedures for reporting concerns.
  - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
  - will be made aware of how the school will monitor policy compliance by: ensuring staff are fully trained and well equipped to deal with policy breaches and know their responsibility online by agreeing to the AUPs in place at both schools. These will be monitored by the IT technician and all staff are expected to remain vigilant for any potential issues.
  - are expected to adopt a partnership with the school to resolve issues.
- If appropriate, after any investigations are completed, the DSL and 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 headteacher will seek advice from the local authority or other agency in accordance with our child protection policy. Consult with

Area Education Safeguarding Advisor (Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk or **Online Safety:** Ashley Assiter (Monday/Tuesday/Wednesday) - 03301 651 500

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

7.1 Concerns about learner online behaviour and/or welfare

- All concerns about learners will be responded to and recorded in line with our child protection policy:
  - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
  - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or 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.

7.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Executive Headteacher/Head of School, 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). The **LADO** Team: **03000 41 08 88** or email kentchildrenslado@kent.gov.uk.
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

7.3 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 and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

8. Procedures for Responding to Specific Online Concerns

8.1 Online child on child abuse

- Lydden and River Primary Schools Federation recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse other children; all online child on child abuse concerns will be responded to in line with our child protection, behaviour and anti-bullying policies.
- We recognise that online child on child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
  - initiation/hazing type violence and rituals.
- Lydden and River Primary Schools Federation believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- Lydden and River Primary Schools Federation believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- Lydden and River Primary Schools Federation recognises that, even if there are no reported cases of online child on child abuse, such abuse is still likely to be taking place.
- Concerns about learner's behaviour, including child on child abuse taking place online offsite will be responded to as part of a partnership approach with learners and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies.
- Lydden and River Primary Schools Federation want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child on child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Learners who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Lydden and River Primary Schools Federation will follow the guidance outlined in Part Five of KCSIE 2023 and the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' guidance.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression

that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.

- Lydden and River Primary Schools Federation recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- Lydden and River Primary Schools Federation recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and 24 services, and for things to move from platform to platform online.
- Lydden and River Primary Schools Federation 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.
- Lydden and River Primary Schools Federation 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum. Our relationships education, part of our PSHE curriculum ensure children learn how to behave respectfully online. Our computing curriculum also addresses children's responsibility online, including their conduct. Our school values reinforce our expectation that everyone is valued and we behave with responsibility and integrity online.
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children, and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the Police. Consult with Area Education Safeguarding Advisor (Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk
    - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
    - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Following an immediate risk assessment, the school will:

- 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.
- inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- if the concern involves children and young people at a different educational school, 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 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.

- Lydden and River Primary Schools Federation recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Lydden and River Primary Schools Federation also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working will all age groups, not just older learners.

- Lydden and River Primary Schools Federation recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
    - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
    - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
    - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and/or semi-nude imagery, Lydden and River Primary Schools Federation will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- Lydden and River Primary Schools Federation will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods. Through our Sex and relationships education (SRE) curriculum, children are taught 'pants are private' in KS1 and rules around

appropriate contact. In KS2 children are taught about privacy in more detail including about the rules for conduct, content and contact online.

- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
  - Report any concerns to the DSL immediately.
  - Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
  - Not delete the imagery or ask the child to delete it.
  - Not say or do anything to blame or shame any children involved.
  - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
  - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
  - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
  - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
  - a referral will be made to Children's Social Care and/or the police immediately if:
    - the incident involves an adult (over 18).
    - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
    - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
    - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
  - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
  - If DSLs are unsure how to proceed, advice will be sought from the local authority. Consult with Area Education Safeguarding Advisor (Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk
  - Store any devices 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.
  - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
  - provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
  - implement sanctions where necessary and appropriate 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.
        - Learners will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
    - 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.
- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. Note, DSLS should follow: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, 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 and will not allow or request learners to do so.

10.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Lydden and River Primary Schools Federation.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.2 Online child abuse and exploitation

- Lydden and River Primary Schools Federation 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, in line with our child protection policy.
- Lydden and River Primary Schools Federation 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. The computing and PSHE curriculum support teachers to address issues regarding exploitation.
- 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.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant local safeguarding children partnership 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. Consult with Area Education Safeguarding Advisor

(Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk
    - 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 school 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 the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police. Consult with Area Education Safeguarding Advisor (Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk
- We will ensure that the NCA-CEOP reporting tools are visible and available to learners and other members of our community. On the school website and AUPS for children.
- 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.
- If members of the public or learners at other schools are believed to have been targeted, the DSL, will seek advice from the police and/or the Local Authority before sharing specific information to ensure that potential investigations are not compromised. Consult with Area Education Safeguarding Advisor (Dover - 03301 651 340) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk

10.3 Indecent Images of Children (IIOC)

- Lydden and River Primary Schools Federation will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- 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 will obtain advice immediately through the police and/or the Local Authority. Consult with Area Education Safeguarding Advisor (Dover - 03000 423 154) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures. Consult with Area Education Safeguarding Advisor (Dover - 03000 423 154) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk

    - store any devices involved securely, until advice has been sought. If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by learners.
    - report concerns as appropriate to parents and carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL 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 any other agencies, 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, we will:
    - ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police in accordance with our managing allegations against staff policy.
    - quarantine any involved school provided devices until police advice has been sought.

10.4 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Lydden and River Primary Schools Federation 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 will obtain advice through the Local Authority and/or the police. Consult with Area Education Safeguarding Advisor (Dover - 03000 423 154) or Local Authority Social Worker at the Front Door: www.kscmp.org.uk

10.5 Online radicalisation and extremism

- 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 will be informed immediately, and action will be taken in line with our child protection policy:

- If the concerns relate to a member of staff, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

10.6 Cybercrime

- Lydden and River Primary Schools Federation recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

9. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 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
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
  - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk

10. Appendix 1

Local Support

- All members of staff in Lydden and River Primary Schools Federation are made aware of local support available.

If a child may be at risk of imminent harm, call the Integrated Front Door on 03000 411 111 (outside office hours - 03000 419 191) or the Police on 999

- **Education Safeguarding Service**
  - **Area Safeguarding Advisor**
  - **Dover** - 03000 423 154
  - **Online Safety in the Education Safeguarding Service**
    - 03000 423164
    - onlinesafety@kent.gov.uk **(non-urgent issues only)**

- **LADO Service**
  - **03000 410888**
  - kentchildrenslado@kent.gov.uk
- **Kent Integrated Children's Services/ Children's Social Work Services**
  - Front Door: 03000 411111
  - Out of Hours Number: 03000 419191

- **Early Help**
  - www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-and-preventative-services and www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

- **Kent Police**
  - 101 or 999 if there is an immediate risk of harm

- **Kent Safeguarding Children Multi-Agency Partnership (KSCMP)**
  - www.kscmp.org.uk
  - 03000 421126 or kscmp@kent.gov.uk

- **Adult Safeguarding**
  - Adult Social Care via 03000 41 61 61 (text relay 18001 03000 41 61 61) or email social.services@kent.gov.uk

Appendix 2

Appropriate Filter Provider Response

https://d1xsi6mgo67kia.cloudfront.net/uploads/2022/07/Smoothwall-Appropriate-Filtering-Provider-Response-2023.pdf