# Online Safety Policy

**Vision Statement**

Our Ospringe School family's Christian Ethos of Nurture-Grow-Succeed is underpinned by Jesus' Parable of the Mustard Seed. We nurture a joyful, family-centred community where all feel rooted, valued and inspired. Through play and exploration, we foster curiosity, confidence and a lifelong love of learning. Our strong, effective curriculum embraces the richness of Faversham and the wider world. We empower our children to become stewards of creation and be vocal advocates for themselves and others. We create a safe, warm, inclusive nest in our nurturing branches, where children grow in kindness, resilience and wonder ready to flourish as compassionate individuals.






**Our Christian Values**

Compassion
Forgiveness
Equality
Honesty
Perseverance
Courage

| Policy Review | | |
|---|---|---|
| Last Review | Approved by GB | Next Review Due |
| September 2026 | September 2026 | September 2027 |

# 1. Policy Aims and Scope

- This online safety policy has been written by Ospringe CE Primary School, involving staff, learners and parents/carers, building on Kent County Councils LADO and Education Safeguarding Advisory Service 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 Kent Safeguarding Children Board 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.
- Ospringe CE Primary School understands the 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: child to child 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 explicit images and online bullying.
    - **Commerce**: risks online such as gambling, inappropriate advertising, phishing or financial scams.

- Ospringe CE Primary School 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 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).
- Ospringe 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 Code of conduct
- Behaviour policy
- Child protection policy
- GDPR and Data Protection policy
- Curriculum policies
- Use of Images policy
- Mobile and smart technology and social media policies
- AI Use In School policy

## 2. Responding to Emerging Risks

- Ospringe CE Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - 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.
  - 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. Policy monitoring and review

- Technology evolves and changes rapidly. Ospringe will review this policy at least annually. The policy will 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. Any issues identified will be incorporated into our action planning.
- 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.
- All members of the community will be made aware of how our school will monitor policy compliance: AUPs, Staff Training, Online Safety Teaching and classroom management

## 4. Roles and Responsibilities

## 4.1 Headteacher and senior leaders

- The governing body have a strategic leadership responsibility for our school's online safeguarding arrangements; they will ensure that they comply with their duties under legislation and will ensure the policies, procedures and training in our school is effective and comply with the law at all times. (name), headteacher/principals will ensure that the online safety policies and procedures, adopted by our governing bodies and proprietors, are understood, and followed by all staff.
- The Designated Safeguarding Lead (DSL) (Amanda Ralph, Headteacher) has overall responsibility for the day-to-day oversight of safeguarding and child protection systems, including online safety and understanding the filtering and monitoring systems and processes in place. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for online safety remains with the DSL and this responsibility will not be delegated.
- Whilst the DSL is recognised as holding overall lead responsibility for online safety, however Ospringe recognises that all members of the community have important roles and responsibilities to play with regards to online safety.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

## 4.2 Leadership & Management

- 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 the DSL and Primary Technologies to ensure that suitable and appropriate filtering and monitoring systems are in place but hold overall responsibility for procuring our filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of our provision and overseeing any reports.

- 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.

## 4.3 Governors

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee**.**
- Undertake basic cyber security awareness training and support school cyber security oversight.

## 4.4 The Designated Safeguarding Lead (DSL):

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

- The 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.
    - Taking lead responsibility for overseeing and acting on any concerns identified by our filtering and monitoring systems.
    - 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.

## 4.5 Members of Staff

- 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 e.g. Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.
- Staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- Staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- Staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles
- Staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- Staff follow cyber security policy and requirements.

## 4.6 IT Staff/IT Service Providers

- It is the responsibility of Primary Technologies who are managing our technical environment to:
    - Provide technical support and perspective to the DSL and leadership team in the development and implementation of our online safety policies and procedures, including appropriate filtering and monitoring systems.
    - Support the leadership team and DSL to procure systems, identify risk, carry out reviews and carry out checks to our filtering and monitoring systems.
    - Whilst responsibility for the procurement and implementation of appropriate filtering and monitoring is held by the leadership team and responsibility for acting on safeguarding concerns is led by the DSL; technical staff will 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.
    - Implement appropriate security measures 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.

## 4.7 Pupils/Students

- 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.
  - Use AI responsibly: protect original work, check accuracy and avoid plagiarism.

### 4.8 Parents & Carers

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 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

- Ospringe 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 and Sex Education, Health Education, PSHE 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 through the use of our 'Web Warrior' group of online safety representatives.
    - 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.
    - providing online safety education as part of the transition programme across the key stages and when moving between establishments.
    - rewarding positive use of technology.

- Ospringe 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.
    - collaboratively creating a class charter, documenting strategies for following online safety
    - 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.

- Ospringe 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.

- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

## 5.2 Vulnerable Learners and those who are potentially at greater risk of harm

- Ospringe 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.
- Ospringe will ensure that differentiated and appropriate online safety education, access, and support is provided to all learners who require additional or targeted support.
- Staff at Ospringe will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher and Computing Lead 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 carried out as part of existing annual safeguarding and child protection training.
  - 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

- Ospringe 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. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach.
- 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 and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - 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 welcome to school packs.
    - requiring them to read our acceptable use of technology policies and discuss the implications with their children.
    - clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches
    - accurate, balanced and age-appropriate information about changes affecting social media and other online services
    - guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
    - guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
    - mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

## 6 Safer Use of Technology

### 6.1 Classroom use

- Ospringe 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, remote learning platform/tools and intranet
    - Email
    - Games-based technologies
    - Digital cameras, web cams and video cameras

- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- 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.
- Supervision of learners will be appropriate to their 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.

- 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.
- We will ensure that the use of internet-derived materials by staff and learners complies with copyright law and acknowledge the source of information.

### 5.2 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.

## 7 Appropriate Filtering and Monitoring on School Devices and Networks

## 7.1 Responsibilities for filtering and monitoring

- Our governing board 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.

- Amanda Ralph (headteacher**)** and Barry Hostead (governor) are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.

- Our senior leadership team are responsible for:
    - procuring our 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 Primary technologies have sufficient time and support to manage their filtering and monitoring responsibilities.
    - filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.

- 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.

- Primary Technologies 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, learners and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

- Where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products.
- The technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content.
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.

## 7.2 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 works closely with the DSL and Primary Technologies. Decisions have been recorded and informed by an approach which ensures our systems meet our schools' specific needs and circumstances, including but not limited to our learner 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.
- In addition, our school undertakes 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.
- Our school 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.

## 7.3 Appropriate Filtering

- Ospringe's education broadband connectivity is provided through Primary Technologies (S.E.) LTD and Ospringe uses Watchguard filtering system.
- Watchguard is a member of Internet Watch Foundation (IWF).
- Watchguard has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Watchguard is blocking access to illegal content including child sexual abuse material (CSAM).
- Watchguard 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 school owned, or provided, internet enabled devices and networks.
- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

- We work with Primary Technologies 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 learners or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
    - turn off monitor/screen,
    - report the concern immediately to a member of staff,
    - report the URL of the site to technical staff/services.

- 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 behaviour 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), the police (either via 101 or 999 if an emergency or NCA-CEOP) or Children's Social Care.
- 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 leadership team.

## 7.4 Appropriate monitoring

- We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:
    - physical monitoring (supervision),
    - monitoring internet and web access (reviewing logfile information

- All users will be informed that use of our devices and networks can be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to a learner, 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 behaviour policies.
    - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff code of conduct.
- 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, the Police via 101 or NCA-CEOP , the LADO or Children's Social Care.

## 7.5 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 GDPR policy which can be accessed on our school website.

## 7.6 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.

## 7.7 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.
- All learners are provided with year group log in information to access our systems but have specific individual usernames and passwords to access other programmes.
- We require all users to
    - use strong passwords for access into our system
    - change their passwords every 3 months
    - not share passwords or log in information with others or leave passwords/login details where others can find them
    - not to log in as another user at any time
    - lock access to devices/systems when not in use

## 7.8 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.

## 7.9 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 GDPR, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

## 7.10 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 (Amanda Ralph, Headteacher and DSL)
- 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 (CPOMS) for reporting wellbeing and pastoral issues. This will be managed by designated and trained staff.

## 7.11 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.

## 7.12 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.

## 7.13 Educational use of videoconferencing and/or webcams

- Ospringe 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 and 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.

## 7.14 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 take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, according to the learners age and ability.

- 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.

## 7.15 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.

## 7.16 Management of learning platforms

- Ospringe uses our school website and Google Classroom as its official learning platforms 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.

## 7.17 Management of remote learning

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

- Ospringe 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, e.g. Microsoft Teams.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour policy 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. Ospringe 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.

### 7.18 Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue).

**Ospringe ensures that:**

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

## 8 Responding to Online Safety Risks or Policy Breaches

The school recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child.

- 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.
    - 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:
    - 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, including 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.
- 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/Headteacher will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

## 8.1 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.

## 8.2 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). Telephone: 03000 410888 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.

### 8.3 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.

# 9 Procedures for Responding to Specific Online Concerns

### 8.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Ospringe CE Primary School will follow the guidance outlined in Keeping Children Safe in Education 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 ashamed for making a report.
- Ospringe CE Primary School 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

- Ospringe CE Primary School 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.
- Ospringe CE Primary School 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.
- Ospringe CE Primary School will ensure that all members of our 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 PSHE/RSE and Computing curriculum.
- 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, adult students and staff and any actions that are required to protect them.
    - Reports will be initially manged internally by the DSL, and where necessary will be referred to Children's social care and /or the police.
    - 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 and 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.

- Ospringe CE Primary School recognises that the 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. Ospringe CE Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

## 8.2 Nude or semi-nude image sharing

- Ospringe recognises that consensual and non-consensual sharing of nude or semi-nude image sharing (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue and 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, Ospringe 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'
- Ospringe 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, including an age-appropriate RSE curriculum.
- 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 or 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 shared the imagery by accident, this will immediately be 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 the 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, DSL's will:
  - act in accordance with our child protection policies and the relevant local procedures and in line with 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
  - 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: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
  - 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. DSLs will follow advice from: '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, 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.

## 8.3 Cyberbullying

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

## 8.4 Online child abuse and exploitation

- Ospringe 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.
- Ospringe 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.
- 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.
    - 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.
- We will ensure that the NCA-CEOP reporting tools are visible and available to learners and other members of our community, which can be accessed on our school website.
- 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.

## 8.5 Indecent Images of Children (IIOC)

- Ospringe 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 and specific advice can be accessed via the Education Safeguarding Service
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.
    - 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 report 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 local 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.

## 8.6 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Ospringe 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.

## 8.7 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. EIS will filter and monitor internet use.
- 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.

## 8.8 Cybercrime

- Ospringe CE Primary School 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 being 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
- London Grid for Learning: https://lgfl.net/safeguarding
- 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

**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
- Parent Info: https://parentinfo.org
- 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
- Common Sense Media: www.commonsensemedia.org