CLIFTONVILLE PRIMARY AND PRE-SCHOOL

Independence Safe and Settled Resilience Respect Aspiration Learning Community

OUR MISSION

As an outstanding school we will inspire children to achieve more than they ever believed possible

OUR VISION

That every member of our school community is challenged and supported to be the very best they can be

That through our high-quality learning experiences & curriculum we will improve the life-chances of our children

That we educate the whole child so they can thrive in a changing world

Online Safety Policy

Designated Safeguarding Lead: Helen Davin – Deputy Head Teacher

Governor with lead responsibility – Ellie Matthews

Date written: September 2026

Date agreed and ratified by the Governing Body:

Date of next review: September 2027

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

1. Policy Aims

- This online safety policy has been written by involving specialist staff and Senior Leaders building on the Kent County Council/The Education People guidance.

- 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.

- The purpose of the online safety policy is to:
    - Safeguard and protect all members of the Cliftonville Primary & Pre-School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, and to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- Cliftonville Primary & Pre-School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate, or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commercialism:** being unaware of hidden costs and advertising in apps, games, and websites
    - **Commercialism:** being unaware of hidden costs and advertising in apps, games, and websites

2. Policy Scope

- Cliftonville Primary & Pre-School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Cliftonville Primary & Pre-School identifies that the Internet and associated devices, such as computers, tablets, mobile phones, and games consoles, are an important part of everyday life.
- Cliftonville Primary & Pre-School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents, and carers.
- This policy applies to access to the Internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets, or mobile phones.

2.1 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Child protection policy
- Curriculum policy
- Sex Education (RSE) policy
- Data security
- Coastal Academies Trust Data Protection policy
- Searching, screening and confiscation national guidelines are followed.
- Mobile Technology & Social Media Policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Cliftonville Primary & Pre-School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Designated Safeguarding Lead will be informed of online safety concerns, as appropriate.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The **Designated Safeguarding Lead (DSL)** has responsibility for online safety. (***Note: Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.)
- Cliftonville Primary & Pre-School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and/or acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.

- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local, and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date information required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers, and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies, and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet with the governor with a lead responsibility for safeguarding and/or online safety.
- Meet with the safeguarding team fortnightly or more frequently if necessary.

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.

- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and 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 children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting 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 *(Anti-Virus, Firewalls Web-Filtering and Monitoring)* as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the DSL or deputies to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/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-appropriate online safety education opportunities.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- understand that their child will access the Internet.
- acknowledge that no content filtering system is totally secure.
- understand the school cannot be held responsible for content accessed and is not liable for any damage arising from such access.
- 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.
- identify changes in behaviour that could indicate that their child is at risk of harm online.
- seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- use our systems, such as learning platforms, and other network resources, safely and appropriately, where such access is appropriate.
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies such AI (Artificial Intelligence).

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- Cliftonville Primary & Pre-School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Cliftonville Primary & Pre-School will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- Cliftonville Primary & Pre-School recognises that some learners are more vulnerable online due to a range of factors. This may include, but are not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Cliftonville Primary & Pre-School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners**.**
- When implementing an appropriate online safety policy and curriculum Cliftonville Primary & Pre-School will seek input from specialist staff as appropriate, including the SENDCO, Child in Care Designated Teacher, DSL Team, and Parent Support Advisors.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - This will form part of regular safeguarding updates and following any significant incident.
    - This will cover the potential risks posed to learners **(Content, Contact, Conduct and Commercialism)** as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the community.

5.4 Awareness and engagement with parents and carers

- Cliftonville Primary & Pre-School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
        - This will include offering specific online safety awareness training and highlighting online safety at other events which may include parent evenings, transition events, fetes, and sports days.

- Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreements and AUP.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Cliftonville Primary & Pre-School recognises that the Internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess, and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the Internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- 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 to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Cliftonville Primary & Pre-School uses a wide range of technology. This will or may include access to:
  - Computers, Laptops, Chromebooks, iPads, and other digital devices
  - The Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  - *Examples include, Google Safe Search and Google Classroom, Kid Rex and Safe Search Kids*.

- 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 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.
        - We will balance children's ability to take part in age-appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

7.2 Managing Internet Access

- We will maintain a digital record of users who are granted access to our devices and systems.
- All staff will read and sign an acceptable use policy before being given access to our computer system, IT resources or Internet. Learners will be reminded of their responsibility when accessing school devices and systems. Visitors to the school will be given written safeguarding guidance when signing in.

7.3 Filtering and Monitoring

- As part of the school's Internet provision, market leading filtering and monitoring is used to provide a high level of safeguarding and monitoring.

7.3.1 Decision Making

- Cliftonville Primary & Pre-School Senior Leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The Senior Leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

Appropriate filtering

No filtering system can be 100% effective; schools and colleges need to understand the coverage of their filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet their statutory requirements as identified in KCSIE and the Prevent duty.

Cliftonville Primary and Pre-School's education broadband connectivity is provided through Sota and **Cliftonville Primary and Pre-School** uses **Smoothwall Content Filtering and Monitoring**.
Sota is not a member of Internet Watch Foundation (IWF). Sota have confirmed this "as we do not utilise in-network filtering and also do not host website content."
Smoothwall participates in and blocks content from the Counter-Terrorism Internet Referral Unit list (CTIRU)
Smoothwall participates in and blocks content from Child Sexual Abuse Material (CSAM) lists.
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. **Please note this list is not exhaustive.**

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/college broadband connection.
We work with **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/students or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:

Close the lid of the device, turn off the screen (if separate from the device) and report it to a supervising adult who will in turn report the incident to the IT staff. If the incident is of a more serious safeguarding nature, this should be reported immediately to the **Lead DSL – Helen Davin** or **Graham Clayson** who is a **Deputy DSL** with a focus on Online Safety. In their absence it should be reported to another member of the Safeguarding Team (all of whom are trained DSLs) and recorded on CPOMS.

Filtering breaches will be reported to the **DSL (or a Deputy 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), 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 leadership teams.**

7.3.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
- Physical supervision, historical and real-time monitoring of internet and web access.
- If a concern is identified via monitoring approaches, we will:
    - Follow safeguarding procedures in line with all appropriate policies.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights, and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred, and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in the GDPR privacy notice on the school website.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media 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.
    - Regularly checking files held on our network,
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all ***but the youngest users***. (*Note: this will be in place for all except Early Years and Foundation Stage children and some learners with SEND*)
    - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff will 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 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.

- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, generic email addresses (e.g., *office@cliftonvilleprimary.co.uk*), and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices and guidance, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell ***Claire Whichcord – Head Teacher or Graham Clayson a Deputy DSL (Online Safety)***, if they receive offensive communication, and this will be recorded in our safeguarding files/records, where appropriate.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners, and parents.

7.8.2 Learner email

- Individual pupil email addresses are not provided.
- Whole-class or group email addresses **may be** used for communication outside of the setting.

7.9 Management of Applications and Websites used to Record Children's Progress

- We use several websites and apps to track learners progress and share appropriate information with parents and carers.
- The **Head Teacher** is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment, or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment, or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

- Please refer to our **Mobile & Smart Technology and Social Media Policy**

9. Use of Personal Devices and Mobile Phones

- Please refer to our **Mobile & Smart Technology and Social Media Policy**.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents, and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers, and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we 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 **Lead DSL** will seek advice from the Education Safeguarding Service.
- Where there is suspicion, that illegal activity has taken place, we will contact the Education Safeguarding Service or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the **Lead DSL or deputy** will speak with Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

- The **Lead DSL or deputy** will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The **Lead DSL or deputy** will record these issues in line with our child protection policy.
- The **Lead DSL or deputy** will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the **Head Teacher (Deputy DSL) or Deputy Head Teacher (Lead DSL)**, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the **LADO (Local Authority Designated Officer).**
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" which is now incorporated in part 5 of 'Keeping children safe in education'.
- Cliftonville Primary & Pre-School recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Cliftonville Primary & Pre-School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Cliftonville Primary & Pre-School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Cliftonville Primary & Pre-School will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the **Lead DSL or deputy** and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learner's electronic devices, they will be managed in accordance with the latest DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting, and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other **Lead DSLs** to ensure appropriate safeguarding action is taken in the wider local community.

        - If a criminal offence has been committed, the **Lead DSL or deputy** will discuss this with Kent 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.

11.2 Youth Produced Sexual Imagery ("Sexting")

- Cliftonville Primary & Pre-School recognises youth produced sexual imagery as a safeguarding issue; all concerns will be reported to and dealt with by the **Lead DSL or deputy.**
- We will follow the latest advice as set out in the Sharing nudes and semi-nudes: advice for education settings working with children and young people, published by UK Council for Internet Safety (UKCIS).
- Cliftonville Primary & Pre-School will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of 'sharing nudes and semi-nudes' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding sharing nudes and semi-nudes.
- We will respond to concerns regarding sharing nudes and semi-nudes, regardless of whether the incident took place on site or using school provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the **Lead DSL or a Deputy DSL** and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e.sharing nudes and semi-nudes) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - Ensure the **Lead DSL or deputy** responds in line with the Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance published by the UK Council for Internet Safety (UKCIS).
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved, including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed..

- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Cliftonville Primary & Pre-School will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Cliftonville Primary & Pre-School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the **Lead DSL or deputy.**
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal 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 sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child 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.
    - 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the **Lead DSL or deputy** will obtain advice immediately through the Education Safeguarding Service and/or Kent Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the **Lead DSL or deputy.**
- If learners at other settings are believed to have been targeted, the **Head Teacher or Lead DSL or deputy** will seek support from Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Cliftonville Primary & Pre-School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 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 block list and by implementing appropriate filtering, firewalls, and anti-spam software.
- If we are unclear if a criminal offence has been committed, the Head Teacher/DSL or deputy will obtain advice immediately through Kent Police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the **Lead DSL or deputy** is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on school provided devices, we will:
    - Ensure that the **Lead DSL or deputy** is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - Ensure that the **Head Teacher or deputy** is informed in line with our managing allegations against staff policy.
    - Inform the **Local Authority Designated Officer (LADO)** and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Cliftonville Primary & Pre-School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy available on the school website.

11.6 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Cliftonville Primary & Pre-School and will be responded to in line with existing policies, including 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 **Lead DSL or deputy** will obtain advice through the Education Safeguarding Service and/or Kent Police.

11.7 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.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the **Lead DSL or deputy** will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the **Head Teacher or deputy** will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Cyber Security

Staff will receive training annually or following any breach of security to ensure an updated and consistent approach to the threat of a cyber-attack. This will include but is not limited to, Phishing Emails, Downloads and Ransome Ware. Any activity that is suspicious should immediately be reported to the **IT Staff and/or Head Teacher or their deputies.**

13. Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Service:

- Rebecca Avery, Education Safeguarding Advisor (Online Protection)
- Ashley Assiter, Online Safety Development Officer
    - Tel: 03000 415797
- Guidance for Educational Settings:
    - Child protection and safeguarding - KELSI

KSCB:

- www.kscmp.org.uk

Kent Police:

- www.kent.police.uk

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net

National Links and Resources for Educational Settings

- CEOP:
    - www.ceopeducation.co.uk/professionals/
    - www.ceop.police.uk/Safety-Centre/
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org.uk
- NSPCC: www.nspcc.org.uk/keeping-children-safe/online-safety/
- ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/professionals-online-safety-helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk/

National Links and Resources for Parents/Carers

- Action Fraud: www.reportfraud.police.uk
- CEOP:
  - www.ceopeducation.co.uk/parents
  - www.ceop.police.uk/Safety-Centre/
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org.uk
- NSPCC: www.nspcc.org.uk/keeping-children-safe/online-safety/
  - ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk