Online Safety Policy

1.Policy Aims

- This online safety policy has been written by Rainbow Pre-school involving staff and parents/carers, building on the Kent County Council (KCC)/The Education People online safety policy template dated November 2018, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2018, Early Years and Foundation Stage 2017 and the Kent Safeguarding Children Multi-agency Partnership procedures.

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

- Rainbow Pre-school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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.

2.Policy Scope

- Rainbow Pre-school believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Rainbow 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.
- Rainbow 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 committee, practitioners, 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) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
    - Acceptable Use Policies (AUP)
    - Behaviour policy (particularly regarding anti-bullying)
    - Staff Code of Conduct
    - Child protection policy
    - Confidentiality policy
    - Data security
    - Use of Mobile Phones & Cameras
    - Image Use Policy
    - Social Network Acceptable Use Policy

3.Monitoring and Review

- Technology in this area evolves and changes rapidly. Rainbow 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 manager will be informed of online safety concerns, as appropriate.

- Any issues identified will be incorporated into the action planning.

4.Roles and Responsibilities

- The pre-school has appointed Sandra Burgess (Designated Safeguarding Lead) to be the online safety lead.
- Rainbow Pre-school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

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 an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Online Safety Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school 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.

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 DSL's to ensure online safety is recognized as part of the settings safeguarding responsibilities and 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 the relevant up to date knowledge required to keep learners safe 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 schools 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 manager and Committee
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

- Meet regularly (once a term) with Committee member responsible for safeguarding and online safety

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 AUPs.
- Take responsibility for the security of school 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 school's 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.

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 password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.
- Ensure appropriate access and technical support is given to the DSL and deputy DSL to our filtering and monitoring systems, to enable them to take appropriate safeguarding action

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- 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.

It is the responsibility of parents and carers to:

- Support our online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behavior 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.

- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5.Education and Engagement Approaches

Education and engagement with learners

Please note that the educational programmes that the children can access are downloaded and the children do not have access to the internet on the computer or the ipad. If the internet is accessed in the classroom it will be for educational purposes and carried out by a member of staff who will be responsible for ensuring the children are not able to access the internet by themselves ie ensure wi-fi is turned off on the ipad and they log off the computer when they are finished.

The staff will be positive role models and raise awareness and promote safe and responsible internet use amongst pupils when an opportunity arises by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Reinforcing online safety messages whenever technology or the internet is in use.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy 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 cover the potential risks posed to learners (Content, Contact and Conduct) 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 school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- 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 school community.

Awareness and engagement with parents and carers

- Rainbow Pre-school recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school 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 the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our school
    - Requiring them to read the school AUP and discuss its implications with their children.

6.Reducing Online Risks

- Rainbow 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 school 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 school community are made aware of the school's 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 the school's AUP and highlighted through a variety of education and training approaches.

7.Safer Use of Technology

Classroom Use

- Rainbow Pre-school uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning Journal Platform
    - 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 AUP 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 such as recommended for schools such as *SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search*, following an informed risk assessment, to identify which tool best suits the needs of our community.
- 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 pupils 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 only to specific and approved online materials, which supports the learning outcomes planned for the learner's age and ability.

Managing Internet Access

- All staff will have access to the pre-school devices and systems but only the manager and deputy will have access to the office computer and administrating platforms for Tapestry and Internet security
- All staff and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

Filtering and Monitoring

<u>Decision Making</u>

- Rainbow Pre-school committee and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The committee and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children 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; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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.

Filtering

- Education broadband connectivity is provided through TalkTalk
- We use Bullguard on classroom computer, laptop uses XperiaSecurity, office computer & iPads have in built security by Apple and the Amazon Hudls have own security which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Internet Service Provider/Filtering Provider to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites
    - The member of staff will report concern (including the URL of the site if possible) to the DSL (or deputy).
    - The breach will be recorded and escalated as appropriate
    - Parent/carers will be informed of filtering breaches involving their child
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - physical monitoring (supervision)
- If a concern is identified via monitoring approaches, we will raise concern with DSL who will respond in line with the child protection policy
- 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.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Information Sharing Policy.

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.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found in our Acceptable Use Policy, Image Use and Using Mobile Phone and Cameras Policies

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.
- We require all users to:
  - Use strong passwords for access into our system.
  - Changing their passwords annually is recommended
  - 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.

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 the 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 the school website for members of the community.

Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Use of Mobile Phones & Cameras, Image Use, Information Sharing, Social Media and AUPs.

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 and AUPs.
  - 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 school community will immediately tell DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted

Staff E-mail

- The use of personal email addresses by staff for any official setting business is not permitted.
  - All members of staff are provided with a specific setting 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 and parents.

Management of Applications (apps) used to Record Children's Progress

- We use Tapestry to track learners progress and share appropriate information with parents and carers.
- The manager 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
- In order to safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store children's 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 children's 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

Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Rainbow Pre-school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Rainbow Pre-schools community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of Rainbow Pre-school's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control staff access to social media whilst using setting provided devices and systems on site.
    - The use of social media during setting hours for personal use **is not** permitted.
    - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Rainbow Pre-school's community on social media, should be reported to the DSL and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within setting.

- Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites as strictly as they can.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Rainbow Pre-school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with the setting's policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or current or past learners' family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and the manager

- Staff will not use personal social media accounts to make contact with learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead (or deputy)

Official Use of Social Media

- *Rainbow Pre-school's* official social media channels are:
  - Facebook page - https://www.facebook.com/Rainbowpreschoolknockholt/
  - Instagram page
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Manager.
  - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage any official school social media channels.

    - Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Use of Mobile Phones and Cameras Policy, Image Use, Data protection, Confidentiality and Child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Sign the school's Social media acceptable use policy.
    - Always be professional and aware that they are an ambassador for the setting.
    - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead (or deputy) and the Manager of any concerns, such as criticism, inappropriate content or contact from learners.

9.Use of Personal Devices and Mobile Phones

- Rainbow Pre-school recognises that personal communication through mobile technologies is an accepted part of everyday life for leaners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as : Anti-bullying, Behaviour, Staff Code of Conduct, Use of Mobile Phones and Cameras, Image Use and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

    - All members of Rainbow Pre-school's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Rainbow Pre-school's community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as classroom, outside play areas and toilets.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of Rainbow Pre-school's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene our Staff Code of Conduct, Behaviour or Child protection policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Confidentiality, Child protection, Data security and Use of Mobile Phones & Cameras, Acceptable Use and Image Use Policy.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place in the lockable locker provided and not used in the classroom when children are present.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Manager such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and Manager
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices within specific areas – the office.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectation of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behavior, child protection and image use'

- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead (or deputy) of any breaches of our policy.

Officially Provided mobile phones land devices

- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.
- Setting mobile phone and devices will always be used in accordance with the acceptable use policy and other relevant policies.

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 school 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 DSL (or deputy) 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 DSL or Manager will speak with Kent Police and/or the Education Safeguarding Service first, to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

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

Staff Misuse

- Any complaint about staff misuse will be referred to the Manager according to 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

Online Sexual Violence and Sexual Harassment between Children

- Rainbow Pre-school recognizes that sexual violence and sexual harassment between children

can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualized online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

- Rainbow Pre-school recognizes that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend than the local community and for a victim or alleged perpetrator to become marginalized and excluded from online communities.
- Rainbow Pre-school also recognized the potential for repeated victimization in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies
    - If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting, and removing online content, as well as providing appropriate counselling/pastoral support
    - 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 Police
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider community
        - If a criminal offence has been committed the 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

Youth Produced Sexual Imagery or "Sexting"

- Rainbow Pre-school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Rainbow Pre-school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' 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 youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment
- We will not
    - View any 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 DSL (or deputy) 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 (ie youth produced sexual imagery) and will not allow or request learners to do so

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, the we will:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sextisng in schools and colleges:responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will take action to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learner(s) 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 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 the school's 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 school 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.

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

- Rainbow 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.
- Rainbow 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 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.
    - We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to members of our community.
- If made aware of incident involving online sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Child protection and Safeguarding 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, using setting provided or personal equipment.
    - Where possible learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team 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 DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Rainbow 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 school 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 DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedure.
    - 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 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 the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the 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 setting provided devices, we will:
    - Ensure that the Manager 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.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Rainbow Pre-school.
- Full details of how we will respond to cyberbullying are set out in the Behaviour Policy (includes Anti-bullying)

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Rainbow Pre-school and will be responded to in line with existing policies, including Behabviour (includes Anti-bullying).
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

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 DSL (or deputy) will be informed immediately and action will be taken in line with the child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Manager will be informed immediately, and action will be taken in line with the Child protection and Allegations policies.

See also Useful Links for Educational Settings

Reviewed February 2020

Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, OnlineSafety Development Officer
  - Tel: 03000 415797
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- 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
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.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/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parent/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- 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
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk