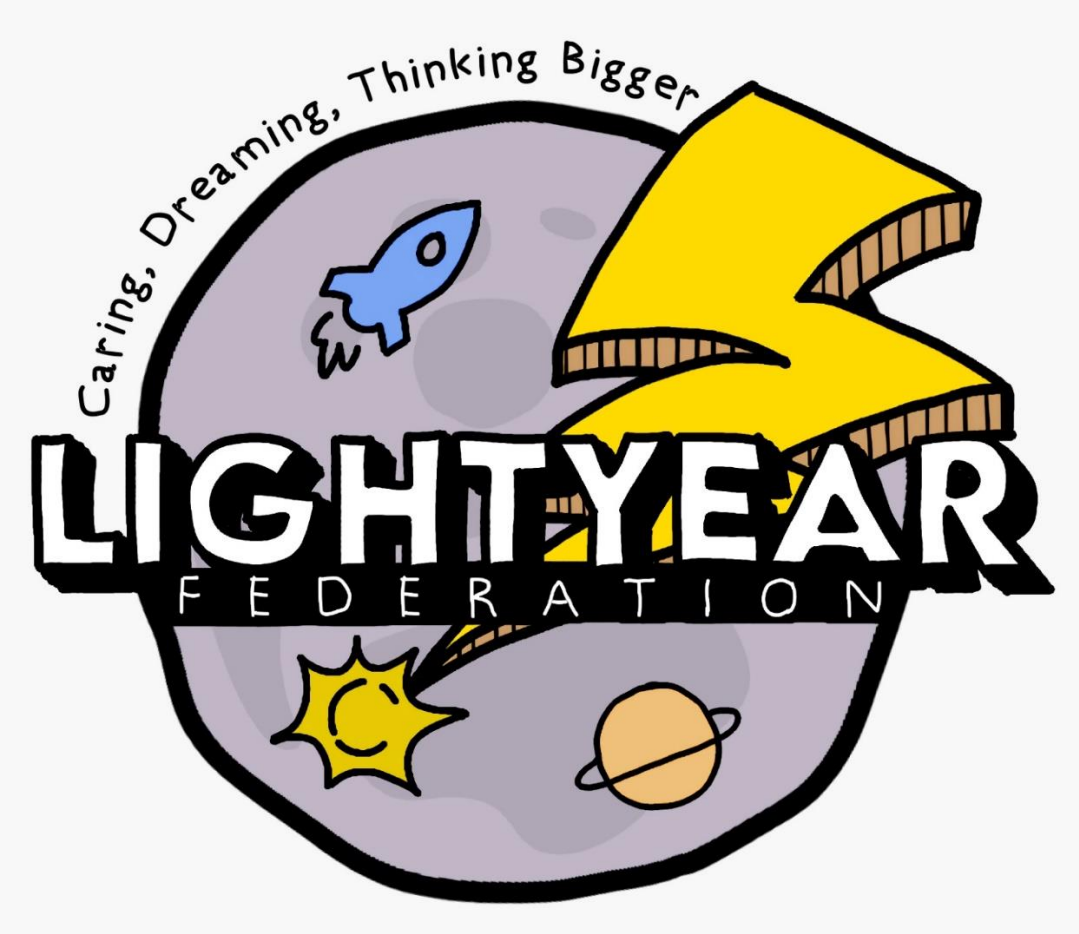

Lightyear Federation Online Safety Policy

September 2024

Policy lead	Hannah Ferris
Date approved by Governing Body	Updated following KCSIE 2024 and awaiting ratification
Review date	September 2025 – or following any updates to national and local guidance and procedures.

Contents

1. Policy Aims and Scope

- This policy has been written by The Lightyear Federation; (Repton Manor Primary School and Greatstone Primary School and Nursery) building on The Education People policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage , 'Working Together to Safeguard Children' and the local Safeguarding Children Multi-agency Partnership procedures.

- The Lightyear Federation recognises that online safety is an essential part of safeguarding and acknowledges our duty to ensure that all children and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole federation approach to online safety which will empower, protect and educate our children and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

- The Lightyear Federation will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.

- The Lightyear Federation understands that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
    - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- The Lightyear Federation recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online.

- This policy applies to children, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy).

- The Lightyear Federation identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

- Staff at The Lightyear Federation recognise that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as being abusive or harmful. This should not prevent staff from having professional curiosity and speaking to a DSL if they have any online safety concerns about a child.

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP)

- Staff code of Conduct
- Behaviour policy
- Safeguarding policy
- Curriculum policies
- Data protection
- Data/information security

2. Responding to Emerging Risks

- The Lightyear Federation recognises that the internet and technology and the risks and harms related to it evolve and change rapidly.
- We will:
  - carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our children face.
  - regularly review the methods used to identify, assess and minimise online risks.
  - examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

- The Lightyear Federation will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- The Executive Headteacher/Head of School will be informed of any online safety concerns by the DSL, as appropriate. The named governors for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the governing body.
- Any issues identified will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Hannah Ferris) is recognised as holding overall lead responsibility for online safety, however Repton Manor Primary School and Greatstone Primary School and Nursery recognises that all members of the community have important roles and responsibilities to play with regards to online safety. The DSL will liaise with other members of staff, for example IT technicians, Computing Leads and leadership teams as necessary.

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

- Hannah Ferris, a member of the senior leadership team and Caroline Allen and David Lea, governors, are responsible for ensuring that our school/college has met the DfE Filtering and monitoring standards for schools and colleges.

- Our federation leadership team are responsible for
  - procuring filtering and monitoring systems.
  - documenting decisions on what is blocked or allowed and why.

- reviewing the effectiveness of our provision.
- overseeing reports.
- ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- ensuring the DSL and IT service providers have sufficient time and support to manage their filtering and monitoring responsibilities.
- Creating a whole school culture that incorporates online safety throughout.
- Ensuring that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies which address the acceptable use of technology, child on child abuse, use of social media and mobile technology.
- Ensure that staff, children and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all children to develop an appropriate understanding of online safety.

- The DSL has lead responsibility for overseeing and acting on:
  - any filtering and monitoring reports.
  - any child protection or safeguarding concerns identified.
  - checks to filtering and monitoring system.
  - acting as a named point of contact on all online safeguarding issues.
  - liaising with other members of staff, such as pastoral support staff, IT technicians, and the Inclusion Team on matters of online safety as appropriate.
  - ensuring referrals are made to relevant external partner agencies, as appropriate.
  - working alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities, and that a coordinated whole school approach is implemented.
  - accessing regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep children safe online, including the additional risks that children with SEN and disabilities (SEND) face online.
  - ensuring all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
  - keeping up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
  - working with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
  - ensuring that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
  - maintaining records of online safety concerns as well as actions taken, as part of the schools safeguarding recording mechanisms.
  - monitoring online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
  - reporting online safety concerns, as appropriate, to the senior leadership team and Governing Body.
  - working with the leadership team to review and update online safety policies on a regular basis (at least annually).
  - meeting regularly with the governors with a lead responsibility for safeguarding.

- All staff are responsible for:
  - contributing to the development of our online safety policies.
  - reading and adhering to our online safety policy and acceptable use of technology policies.
  - taking responsibility for the security of IT systems and the electronic data they use or have access to.
  - modelling good practice when using technology with children.

- maintaining a professional level of conduct in their personal use of technology, both on and off site.
- delivering online safety education within the curriculum wherever possible.
- having an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- identifying online safety concerns and take appropriate action by following our safeguarding policies and procedures.
- knowing when and how to escalate online safety issues, including reporting to the DSL and signposting children and parents/carers to appropriate support, internally and externally.
- Taking personal responsibility for professional development in this area.

- The IT service providers have technical responsibility for:
  - maintaining filtering and monitoring systems.
  - providing filtering and monitoring reports.
  - completing technical actions identified following any concerns or checks to systems.
  - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- It is the responsibility of children (at a level that is appropriate to their individual age and ability) to:
  - engage in age/ability appropriate online safety education.
  - contribute to the development of online safety policies.
  - read and adhere to the acceptable use of technology and behaviour policy.
  - respect the feelings and rights of others, on and offline.
  - take an appropriate level of responsibility for keeping themselves and others safe online.
  - seek help from a trusted adult, if they are concerned about anything, they or others experience online.

- It is the responsibility of parents and carers to:
  - read our Acceptable Use of Technology Policy and encourage their children to adhere to them.
  - support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
  - role model safe and appropriate use of technology and social media and abide by the acceptable use of technology policies.
  - seek help and support from the school or other appropriate agencies if they or their child encounter online issues.
  - use our systems, such as learning platforms and other IT resources, safely and appropriately.
  - take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

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

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

5. Education and Engagement Approaches

5.1 Education and engagement with children

- The Lightyear Federation will work to establish and embed a whole federation culture and will empower our children to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

- We will raise awareness and promote safe and responsible internet use amongst children by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance. The framework for our curriculum is taken from Project Evolve.
    - reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
    - creating a safe environment in which all children feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any children who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our children.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
    - providing online safety education as part of the transition programme across the key stages.
    - rewarding positive use of technology through our behaviour system.

- The Lightyear Federation will support children to understand and follow our Acceptable Use Policy in a way which suits their age and ability by:
    - devising child-friendly versions of our acceptable use policy with the children.
    - displaying acceptable use posters in all rooms with internet access.
    - informing children that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
    - seeking a learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- The Lightyear Federation will ensure children develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.
    - enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - teaching children to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
    - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
    - preparing them to identify possible online risks and make informed decisions about how to act and respond.
    - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable children

- The Lightyear Federation recognises that any children can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some children, for example, looked after children, child who are care leavers, children who are adopted, children who are, or who are perceived to be, lesbian, gay, bi, or trans (LGBT), and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.
- The Lightyear Federation will ensure that differentiated and appropriate online safety education, access and support is provided to all children who require additional and/or targeted support.
- Staff within The Lightyear Federation will seek input from specialist staff as appropriate, including the DSL, Inclusion Team and teaching teams to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- The Lightyear Federation will:
    - provide and discuss the online safety policy and procedures, including our acceptable use policy, with all members of staff, including governors as part of induction.
    - provide up-to-date and appropriate training for all staff including governors, which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be delivered at induction and updated annually as part of our existing annual safeguarding and child protection training/updates, which will, amongst other things, provide them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring
    - provide ongoing online safety training and updates for all staff which will be integrated, aligned and considered as part of our overarching safeguarding approach.
    - ensure our training for governors equips them with the knowledge to provide strategic challenge to test and assure themselves that our online safety policies and procedures in place in are effective and support the delivery of a robust whole school approach.
    - ensure staff training covers the potential risks posed to children (content, contact, commerce and conduct) as well as our professional practice expectations.
    - build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
    - ensure staff are aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
    - ensure staff are aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
    - highlight useful educational resources and tools which staff could use with children.
    - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving children, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- The Lightyear Federation recognises that parents and carers have an essential role to play in enabling our children to become safe and responsible users of the internet and associated technologies.
- We will ensure parents and carers understand and are aware of:
    - the systems used at school to filter and monitor their child's online use by providing information in our Acceptable Use Policy
    - what their children are being asked to do online, including the sites they will asked to access and be clear who from the school (if anyone) their child is going to be interacting with online through our Class Newsletters (Repton Manor Primary School) and Class Dojo (Greatstone Primary School and Nursery).

- We will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential benefits and risks and to reinforce the importance of children being safe online by:
    - providing information and guidance on online safety in a variety of formats.
    - drawing attention to our online safety policy and expectations in our newsletters and other external communication as well as on our website.
    - requesting parents and carers read online safety information as part of joining our community.
    - requiring them to read our acceptable use of technology policies and discuss the implications with their children.

- The Lightyear Federation will ensure parents and carers understand what systems are used to filter and monitor their children's online use through our Acceptable Use Policy.

- Where the federation is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response.

6. Safer Use of Technology

6.1 Classroom use

- The Lightyear Federation uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices
    - Internet, which may include search engines and educational websites
    - Learning platforms, remote learning platform/tools and intranet
    - Email
    - Digital cameras, web cams and video cameras.
- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- Users will be provided with their own account log in details which they will need to use to access laptops and computers.
- iPads do not allow for individual user accounts and therefore will be signed in and out by the child using them.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Staff will use age appropriate search tools with learners and will model safe-searching (e.g. pre-checking searches before displaying the results publicly to learners)
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place.
- We will ensure that the use of internet-derived materials by staff and children complies with copyright law and acknowledge the source of information.
    - Supervision of internet access and technology use will be appropriate to children's age and ability. This includes:
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the children's age and ability.
    - **Key Stage 2**
        - Children will use age-appropriate search engines and online tools.
        - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the children age and ability.

6.1 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role.
- We will maintain a record of users who are granted access to our devices and systems.

6.2 Filtering and monitoring

6.3.1 Decision making

- The Lightyear Federation will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- The Lightyear Federation governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Any changes to the filtering and monitoring approaches will be risk assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team and other relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard children; effective classroom management and regular education about safe and responsible use is essential.
- Our federation undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.
- In addition, our federation undertakes regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the governing body that we are meeting our safeguarding obligations.
    - These checks are achieved by:
        - **Test Filtering** to check filtering systems
        - Tests will be conducted monthly by a DSL. Checks are undertaken with two members of staff present (e.g. a DSL and a member of IT staff and/or a member of SLT), checks are undertaken in a location where confidentiality can be achieved, during working hours, when pupils/students are not present, checks are undertaken on a range of devices/accounts to test different filtering policies and device configurations, checks are logged/recorded, any technical concerns are flagged to the IT staff/IT service provider and safeguarding concerns are actioned by the DSL etc.in line with this policy

6.3.2 Appropriate filtering

- We filter internet use on all federation owned, or provided, internet enabled devices and networks. This is achieved by:
    - Our filtering system being operational, up to date and applied to all users, including guest accounts, all federation owned devices and networks, and all devices using the federation broadband connection.
    - A daily report on the filtering system is provided to the DSL and ICT Technician to allow the DSL to identify device names or IDs, IP addresses, and where possible, individual users, the time and date of attempted access and the search term or content being blocked.
    - iPads will be signed in and out using paper records to enable users to be identified as individual log-ins are not available on these devices.

- The Lightyear Federation's education broadband connectivity is provided through Broadband 4 (Part of PSD Group) and uses Netsweeper as the filtering system.
    - Netsweeper blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes but is not limited to 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.
    - Newtsweeper is a member of Internet Watch Foundation (IWF) and is blocking access to illegal content including child sexual abuse material (CSAM).
    - Netsweeper has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
    - Netsweeper integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' in line and is fully compliant with PREVENT duty.
- We work with Broadband4 and Netsweeper to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If there is failure in the software or abuse of the system, for example if learners or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
    - Lock the computer screen and either take the device to a DSL/Member of SLT or ask for a member of staff to wait with the computer whilst a DSL/member of SLT arrives. The URL will be reported to the ICT technician.
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate in line with existing policies, including child protection, acceptable use and behaviour.
- Parents/carers will be informed of filtering breaches involving children.
- 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 via the Kent Integrated Children's Services Portal.
- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

6.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all federation owned or provided internet enabled devices as necessary. This will be achieved through physical monitoring/supervision and monitoring internet and web access through a regular review of the logfile information.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to children, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour.
    - Where the concern relates to staff, it will be reported to the headteacher or DSL (or chair of governors if the concern relates to the headteacher), in line with our staff code of conductand allegations policy.
- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.

6.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with UK General Data Protection Regulations (UK GDPR) and Data Protection legislation.

6.5 Information security and access management

- The Lightyear Federation is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems, as well as our staff and children.
- To ensure we keep our technical environment safe we ensure:
    - 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
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
    - Checking files held on our network, as required and when deemed necessary by leadership staff.
    - The appropriate use of user logins and passwords to access our network and user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.
- Hannah Ferris, a member of the senior leadership team and Caroline Allen and David Lea, governors, are responsible for ensuring that our federation has met the DfE cyber security standards for schools and colleges.

6.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- Children's passwords are age appropriate throughout the school and there is specific curriculum learning around privacy.
- We require all users to
    - use strong passwords for access into our system.
    - change their passwords periodically
    - not share passwords or login information with others or leave passwords/login details where others can find them.
    - not to login as another user at any time.
    - lock access to devices/systems when not in use.

6.6 Managing the safety of our website

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

6.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies.

6.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/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.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately report offensive communication to a school DSL.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

6.8.1 Staff email

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

6.8.2 Learner email

- Children will:
    - use a provided email account for educational purposes.
    - agree an Acceptable Use Policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.9 Educational use of videoconferencing and/or webcams

- The Lightyear Federation recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

6.9.1 Users

- Parents/carers will be made aware of any videoconferencing and will have a right to withdraw their child from the video.
- Children will ask permission from a member of staff before making or answering a video conference call or message.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, according to the children's age and ability.
- The unique login and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

6.9.2 Content

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

6.10 Management of learning platforms

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

6.11 Management of applications (apps) used to record progress

- Repton Manor Primary School uses Tapestry to track children's progress in EYFS and share appropriate information with parents and carers where needed.
- Greatstone Primary School and Nursery uses Class Dojo to share appropriate information with parents and carers where needed.
- The Executive Head teacher and/or Head of School will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - only learner issued devices will be used for apps that record and store children' 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' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

6.12 Management of remote learning

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

7. Social Media

7.1 Expectations

- The Lightyear Federation believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline and all members of our community are expected to engage in social media in a positive and responsible manner.
- All members of our community are expected to engage in social media in a positive and responsible manner and are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all federation provided systems.
- Concerns regarding the online conduct of any member of The Lightyear Federation community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, staff behaviour/code of conduct, Acceptable Use Policies, and child protection.

7.2 Staff use of social media

- The use of social media during school hours for personal use is only permitted for staff within the staff room during allocated break time.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

7.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the federation. Civil, legal or disciplinary action may be taken if staff are found

to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
  - Setting appropriate privacy levels on their personal accounts/sites.
  - Being aware of the implications of using location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Using strong passwords.
  - Ensuring staff do not represent their personal views as being that of the federation.
- Members of staff are encouraged not to identify themselves as employees of Repton Manor Primary School/Greatstone Primary School and Nursery or the Lightyear Federation on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- Information and content that staff members have access to as part of their employment, including photos and personal information about children 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.

7.2.2 Communicating with children and their families

- Staff will not use any personal social media accounts to contact children or their family members.
- All members of staff are advised not to communicate with or add any current or past children or their family members, as 'friends' on any personal social media accounts.
- Any communication from children and parents/carers received on personal social media accounts will be reported to the DSL (or deputy).
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and/or Executive Headteacher/Head of School.
- If ongoing contact with children is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

7.3 Children' use of social media

- The use of social media during school hours for personal use is not permitted for children.
- Many online behaviour incidents amongst children and young people occur on social media outside the school/nursery day and off the schoo/nursery premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another child, could have repercussions for the orderly running of the school/nursery when the child is identifiable as a member of the school/nursery, or if the behaviour could adversely affect the reputation of the school/nursery, action will be taken in line with our behaviour and child protection/online safety policies.
- The Lightyear Federation will empower our children to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our school website
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for children under the required age as outlined in the services terms and conditions.
- Children will be advised:

    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the setting and externally.
- Any concerns regarding children's use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to children as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding children's use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8. Mobile and Smart Technology

Safe use of mobile and smart technology expectations

- The Lightyear Federation recognises that use of mobile and smart technologies is part of everyday life for many children, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the federation community are advised to:
    - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are never permitted to be used in specific areas on site, such as children's changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of The Lightyear Federation community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.
- Staff will only use their mobile phones on school trips in accordance with the trip risk assessment.

8.1 Federation provided mobile phones and devices

- Some members of staff may be issued with a work phone number in addition to their work email address, where contact with staff, children or parents/carers is required outside of opening hours.
- Staff providing formal remote learning will do so using school provided equipment in accordance with our Acceptable Use Policy/remote learning AUP.
- School mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

- Where staff are using school provided mobile phones and devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

8.2 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones , wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant federation policy and procedures, such as confidentiality, child protection, data security staff behaviour/code of conduct and Acceptable Use Policies.
- Staff will be advised to:
  - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times, these must be kept in the class cupboard, a locked drawer or staff room and must not be out around the children without a specific risk assessment.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  - Not use personal mobile or smart technology devices during teaching periods unless permission has been given by the headteacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting children or parents and carers.
  - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL.
- Staff will only use school provided equipment (not personal devices):
  - to take photos or videos of children in line with our image use policy.
  - to work directly with children during lessons/educational activities.
  - to communicate with parents/carers.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Executive Headteacher/Head of School, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

8.3 Children use of mobile and smart technology

- Children will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations.
- Safe and appropriate use of mobile and smart technology will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our safeguarding and relevant specific curriculum policies.
- The Lightyear Federation recognises that for older children, mobile phones may have a part to play in securing pupils' personal safety before and after school and on journeys to and from school.
  - Where these are required, for example for safety reasons when children/young people are transporting to and from school, devices should be turned off and handed into the class teacher/school office in the morning. They can then be collected at the end of day.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

- If parents need to contact children urgently they should phone the school office and a message will be relayed promptly.
- Under no circumstances will pupils be allowed to take mobile phones on school excursions.
- The school accepts no responsibility for any loss or damage whilst the device is on school premises.
- If a child requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the Executive Headteacher and DSL prior to use being permitted.
    - Any arrangements regarding access to personal mobile or smart technology devices in exceptional circumstances will be documented and recorded by the setting.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and/or their parents carers before use is permitted.
- Where children' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.
- Mobile phones and personal devices must not be taken into examinations. Children found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- Any concerns regarding children's use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.

8.4 Screening, searching and confiscation of electronic devices

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

the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
    - If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.
    - Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - Concerns regarding policy breaches by children will be shared with parents/carers as appropriate.
    - Where there is a concern that a child is at risk of harm, we will respond in line with our child protection policy.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.5 Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that mobile phones are used in a safe and appropriate manner around school grounds. This is explained within our leaflet that is provided to visitors to site.
- Mobile phones should not be used in the classrooms or other places where children are present unless with consent of the Executive Head Teacher or Head of School.
- Parents and carers are able to record their children in assemblies etc but are asked not to share the images on social media.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection. This will be emailed to long term contractors by the site manager and shared with volunteers during their induction.
- If visitors require access to mobile and smart technology, for example when working with children as part of multi-agency activity, this will be discussed with the Executive Headteacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the federation. This may include undertaking appropriate risk assessments if necessary.

- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

9. Responding to Online Risks and/or Policy Breaches

- All members of the community:
    - are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

    - are expected to adopt a partnership with the school to resolve issues.
- Where children/pupils/students breach this policy:
    - appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
    - concerns will be shared with parents/carers as appropriate.
    - we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
    - We require staff, parents/carers and children to work in partnership with us to resolve issues.
    - All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Children's parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) or Executive Headteacher/Head of School will seek advice from the local authority, or other agency in accordance with our child protection policy.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL or headteacher will speak with the police or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

9.1 Concerns about learner online behaviour and/or welfare

- The Lightyear Federation recognises that an initial disclosure to a trusted adult may only be the first incident reported, rather than representative of a singular incident and that trauma can impact memory, so children may not be able to recall all details or timeline of abuse. All staff will be aware certain children may face additional barriers to telling someone, for example because of their vulnerability, disability, sex, ethnicity, and/or sexual orientation.
- All concerns about children will be responded to and recorded in line with our child protection policy:
    - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
    - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Abuse that occurs online and/or offsite will not be dismissed or downplayed; concerns will be treated equally seriously and in line with our anti-bullying, behaviour, child protection and online safety policies.
- The Lightyear Federation recognises that the law is in place to protect children and young people rather than criminalise them, and this will be explained in such a way to children that avoids alarming or distressing them.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to children as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

9.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be managed in accordance with our allegations against staff policy/staff code of conduct/behaviour policy.

- Any allegations regarding a member of staff's online conduct that meets the harm threshold will be discussed with the LADO (Local Authority Designated Officer). Any low level concerns will be recorded in line with our Allegations Against Staff Policy and Staff Code of Conduct.
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

9.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

10. Procedures for Responding to Specific Online Concerns

10.1 Online child-on child

- The Lightyear Federation recognises that, whilst risks can be posed by unknown individuals or adults online, children can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online child-on-child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
  - initiation/hazing type violence and rituals.
- The Lightyear Federation adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse and it will never be tolerated or dismissed as "just banter", "just having a laugh", "part of growing up" or "boys being boys"; this can lead to a culture of unacceptable behaviours and can create an unsafe environment for children and a culture that normalises abuse, which can prevent children from coming forward to report it.
- The Lightyear Federation believes that all staff have a role to play in challenging inappropriate online behaviours between children. Staff recognise that some online child-on-child abuse issues may be affected by gender, age, ability and culture of those involved.
- The Lightyear Federation recognises that even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.
- Concerns about child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with children and parents/carers; concerns will be recorded and responded to in line with existing appropriate policies, for example anti-bullying, acceptable use, behaviour and safeguarding policies.

- The Lightyear Federation want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child-on-child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Children who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, The Lightyear Federation will follow the guidance outlined in Part Five of KCSIE.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- The Lightyear Federation recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting'
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- The Lightyear Federation recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services, and for things to move from platform to platform online.
- The Lightyear Federation will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- The Lightyear Federation will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the Police. Our school can also access specific advice via The Front Door.
    - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
    - If content is contained on children' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Following an immediate risk assessment the school will:

    - provide the necessary safeguards and support for all children involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
    - if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
    - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- The Lightyear Federation recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. The Lightyear Federation also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing

- The Lightyear Federation recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
    - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
    - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
    - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and/or semi-nude imagery, The Lightyear Federation will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- The Lightyear Federation will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
    - Report any concerns to the DSL immediately.
    - Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery, this will be immediately reported to the DSL.
    - Not delete the imagery or ask the child to delete it.
    - Not say or do anything to blame or shame any children involved.
    - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
    - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
    - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.

- carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of children involved, including the possibility of carrying out relevant checks with other agencies.
- a referral will be made to Children's Social Care and/or the police immediately if:
  - the incident involves an adult (over 18).
  - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
  - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
  - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
- the DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
- If DSLs are unsure how to proceed, advice will be sought from the local authority.
- Store any devices securely:
  - If content is contained on children' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- provide the necessary safeguards and support for children, such as offering counselling or pastoral support.
- implement sanctions where necessary and appropriate in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
  - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
  - Children will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

- We will not:
  - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
  - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request children to do so.

10.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Lightyear Federation.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy, available on our school website.

10.2 Online child abuse and exploitation

- The Lightyear Federation recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection policy.
- The Lightyear Federation will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target children, and understand how to respond to concerns.

- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for children, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
    - store any devices containing evidence securely:
        - If content is contained on children' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for children, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
    - Where possible and appropriate, children will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to children and other members of our community through our website.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.
- If members of the public or children at other schools or settings are believed to have been targeted, the DSL will seek advice from the police and/or the Local Authority) before sharing specific information to ensure that potential investigations are not compromised.

10.3 Indecent Images of Children (IIOC)

- Repton Manor Primary School and Greatstone Primary School and Nursery will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Local Authority.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.

    - store any devices involved securely, until advice has been sought. If content is contained on children's personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by children.
    - report concerns as appropriate to parents and carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children, we will:
    - ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police in accordance with our managing allegations against staff policy.
    - quarantine any involved school provided devices until police advice has been sought.

10.4 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at The Lightyear Federation, and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police.

10.5 Online radicalisation and extremism

- We will take all reasonable precautions to ensure that children and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy:
    - If the concerns relate to a member of staff, the Executive Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

10.6 Cybercrime

- The Lightyear Federation recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.

- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

11. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 360 Safe Self-Review tool for schools www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

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

Support for children and parents/carers

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