Acceptable Use of Technology Policy
September 2025

Policy lead	Hannah Ferris
Date approved by Governing Body	Updated to reflect KCSIE 2025 and awaiting ratification by Governors
Review date	September 2026 – or following any updates to national and local guidance and procedures.

Contents

Acceptable Use Policy for Learners

Early Years and Key Stage 1

- I understand that the school rules will help keep me safe and happy online.
- I only go online or use the internet when a grown-up is with me.
- I only click on things online when I know what they do. If I am not sure, I ask a grown-up first.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know my school can see what I am doing online when I use school computers and devices.
- If I see something online that makes me feel upset, unhappy, or worried, I will always tell a grown-up.
- I know that if I do not follow the rules, my parents/carers will be told and I may not be able to use the computers at school.
- I have read and talked about these rules with my teacher and with my parents/carers.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.

Key Stage 2

- I understand that this Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will be kind and respectful online, just like I am at school.
- I only send messages which are polite and friendly.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I only talk with, and open messages, from people I know.
- I will only click on links if a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

- If I bring my own personal smart devices and/or mobile phone to school, I will switch it off and hand it in to my class teacher or to the school office at the beginning of the day. This will be returned to me at the end of the day. I will not use any smart devices and/or mobile phones while I am at school or on school trips.
- I always ask permission from an adult before using the internet.
- I only use websites, tools and search engines that my teacher has chosen and given me

permission to use.
- I use school devices for school work only, unless I have permission otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

Trust
- I know that some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a trusted adult.
- I always credit the person or source that created any work, images, or text I use.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

Responsible
- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them with anyone.
- I will log off when I have finished using a computer or device.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.

Tell
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to an adult in school, or a parent or carer at home.
- If I see anything online that makes me feel worried or upset, I will lock the screen and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to an adult.
- I know it is not my fault if I see something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scare, I will talk to a trusted adult.

Understand
- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are monitored to help keep me safe. This means someone at the school is able to see and check my online activity when I use school devices and networks.
- I have read and talked about these rules with my teacher and my parents/carers.
- I know that I will be able to use the internet in school for a variety of reasons if I use it responsibly. I understand that if I do not, I may not be allowed to use the internet at school.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

Learners with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I know that if I do not follow the school rules then I will not be able to use the computers.

Learners with SEND functioning at Levels P7-L1 (Based on Childnet's SMART Rules)

- I ask a grown up if I want to use the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then I will not be able to use the computers.
- I tell a grown-up if I want to talk on the internet.
- I do not open messages or emails from strangers.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I will tell a grown up.

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules)

- I ask an adult if I want to use the internet.
- I keep my information private on the internet.
- I am careful if I share photos online.
- I know that if I do not follow the school rules then I will not be able to use the computers.
- I tell an adult if I want to talk to people on the internet.
- I talk to an adult if someone online asks to meet me.
- I do not open messages from strangers.
- I check web links to make sure they are safe.
- I make good choices on the internet.
- I check the information I see online.
- I use kind words on the internet.
- If someone is mean online, then I will not reply. I will save the message and show an adult.
- If I see anything online that I do not like, I will tell a grown-up.

Lightyear Federation Acceptable Use of Technology Policy – Learner Agreement

I have read and understood the school Acceptable Use of Technology Policy (AUP) and I agree to follow the AUP when:

I use school devices and systems both at school and at home.

I use my own equipment outside of the school, including communicating

Acceptable Use of Technology for Staff

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Lightyear Federation IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand the Lightyear Federation expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that federation systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services either provided to me by the federation or accessed as part of my role within the Lightyear Federation, both professionally and personally, both on and offsite. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies

2. I understand that the Lightyear Federation's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Safeguarding and Child Protection Policy, Online Safety Policy, and Staff Code of Conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the federation ethos, federation staff code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Federation Devices and Systems

4. I will only use equipment and internet services provided to me by the federation (for example, federation provided computers, laptops, tablets and internet access) when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed (this is used at the federation's discretion and can be revoked at any time).

6. Where I deliver or support remote/online learning, I will comply with the Lightyear Federation remote learning AUP.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

    - I will use a ‘strong’ password to access federation systems and will not disclose my password or security information to others. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
    - I will protect the devices in my care from unapproved access or theft by not leaving devices visible or unsupervised in public places.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report this to the ICT technician***.***

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars or hardware, without permission from the IT system manager.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the federation information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the federation site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the federation. ***Please speak to the IT technician if you need support with this.***
    - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the Federation Data Protection Officer and leadership team prior to use to ensure it is safe and legal.

11. I will not keep documents which contain federation related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the federation learning platform to upload any work documents and files in a password protected environment or federation approved VPN.

12. I will not store any personal information on the federation IT system, including federation laptops or similar device issued to members of staff, that is unrelated to work activities, such as personal photographs, files or financial information.

13. I will ensure that federation owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following

criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. I will not attempt to bypass any filtering and/or security systems put in place by the federation.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT technician and a member of the leadership team as soon as possible.

16. If I have lost any federation related documents or files, I will report this to the ICT Technician and federation Data Protection Officer (Vikki Reeves) as soon as possible.

17. I understand images of learners must always be appropriate and should only be taken with federation provided equipment and taken/published where learners and their parent/carer have given explicit written consent.

Classroom Practice

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented as detailed in our safeguarding and child protection policy and online safety policy, and as discussed with me as part of my induction and ongoing safeguarding and child protection training.

19. If there is failure in the filtering software or abuse of the filtering or monitoring systems, if, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and ICT Technician, in line with the federation safeguarding and child protection policy/online safety policy.

20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the federation safeguarding and child protection/online safety policy.

21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our federation community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that
    - AI tools are only to be used responsibly and ethically, and in line with our federation child protection, data protection, and professional conduct/behaviour policy expectations.

- A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
- A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving children.
- Only approved AI platforms may be used with children.
- Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- Any misuse of AI will be responded to in line with relevant federation policies, including but not limited to, anti-bullying, staff code of conduct, behaviour and child protection policies.

22. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Hannah Ferris) or a deputy DSL as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

23. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

24. I have read and understood the federation online safety policy which covers expectations regarding staff and learners' use of mobile technology and social media.

25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct, the federation online safety policy and the law.

Online communication, including use of social media

26. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policies, staff code of conduct and the law.

27. As outlined in the staff code of conduct and federation online safety policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the federation, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to children, staff, federation business or parents/carers on social media.

28. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via federation approved and/or provided communication channels and systems, such as a federation email address or federation telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
    - If I am approached online by a learner or parents/carer, I will not respond and will report the communication to one of the federation DSLs or Deputy DSLs
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or Executive Head Teacher/Head of School.

Policy Concerns

29. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material or adult pornography covered by the Obscene Publications Act.

30. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

31. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school, nursery or federation into disrepute.

32. I will report and record any concerns about the welfare, safety or behaviour of learners or parents/carers online to the DSL in line with the federation safeguarding and child protection policy.

33. I will report concerns about the welfare, safety, or behaviour of staff online to the Executive Headteacher/Head of School, in line with federation safeguarding and child protection policy and the allegations against staff policy.

Policy Breaches or Concerns

34. If I have any queries or questions regarding safe and professional practise online, either on or off site, I will raise them with the DSL and/or the Executive Headteacher/Head of School

35. I understand that the federation may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of learners and staff. This includes monitoring all federation provided devices and federation systems and networks including federation provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via federation provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

36. I understand that if the federation believe that unauthorised and/or inappropriate use of federation devices, systems or networks is taking place, the federation may invoke its disciplinary procedures as outlined in the staff code of conduct.

37. I understand that if the federation believe that unprofessional or inappropriate online activity, including behaviour which could bring the federation into disrepute, is taking place online, the federation may invoke its disciplinary procedures as outlined in the staff code of conduct.

38. I understand that if the federation suspects criminal offences have occurred, the police will be informed.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the federation community are fully aware of the boundaries and requirements when using any federation Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of the federation community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The federation provides Wi-Fi for the school/nursery community and allows access for education use only.

2. I am aware that the federation will not be liable for any damages or claims of any kind arising from the use a wireless service. The federation takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the federation premises that is not the property of the federation.

3. The use of technology and WIFI falls under Lightyear Federation Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. The federation reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. Federation owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the federation service is adequately secure, such as up-to-date anti-virus software and system updates.

7. Any federation wireless service is not secure, and the federation cannot guarantee the safety of traffic across it. Use of the federation wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The federation accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the federation wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the federation from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10.I will not attempt to bypass any of the federation security and filtering systems or download any unauthorised software or applications.

11.My use of federation Wi-Fi will be safe and responsible and will always be in accordance with the federation AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12.I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the federation into disrepute.

13.I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Hannah Ferris) as soon as possible.

14.If I have any queries or questions regarding safe behaviour online, I will discuss them with the Executive Headteacher/Head of School or DSL.

15.I understand that my use of the federation Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the federation suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the federation may terminate or restrict usage. If the federation suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

The Lightyear Foundation Image Use Policy

1. This policy seeks to ensure that images taken within, and by, The Lightyear Federation are taken and held legally and the required thought is given to safeguarding all members of the community.

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

3. This policy must be read in conjunction with other relevant policies including, but not limited to; safeguarding and child protection, anti-bullying, behaviour, data security, staff code of conduct, and relevant curriculum policies including computing and Relationships, Sex and Health Education (RSHE).

4. This policy applies to all images, including still photographs and video content taken by The Lightyear Federation.

5. All images taken by The Lightyear Federation will be used in a manner respectful of the Data Protection Principles. This means that images will be processed:

- fairly, lawfully and in a transparent manner
- for specified, explicit and legitimate purposes
- in a way that is adequate, relevant limited to what is necessary o to ensure it is accurate and up to date
- for no longer than is necessary
- in a manner that ensures appropriate security

6. The Data Protection Officer (DPO) within The Lightyear Federation (Vikki Reeves, Business Director) supported by the Designated Safeguarding Lead (Hannah Ferris) and leadership team are responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the setting. This includes the management, implementation, monitoring and review of the Image Use Policy.

Official use of images of children

Parental consent

7. Written permission from parents or carers will always be obtained before images of children are taken, used or published.

8. Written consent will always be sought to take and use images offsite for professional, marketing and training purposes. This may be in addition to parental permission sought for onsite images.

9. Written consent from parents will be kept by the school/nursery where children's images are used for publicity purposes, such as brochures or publications, until the image is no longer in use.

10. Parental permission will be sought on admission to school/nursery.

11. A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of, and the record will be updated accordingly.

Safety of images

12. All images taken and processed by or on behalf of the school/nursery will take place using federation provided equipment and devices and in line with this and other associated policies, including but not limited to Safeguarding and Child Protection and the Staff Code of Conduct.

13. Staff will receive information regarding the safe and appropriate use of images as part of their data protection and safeguarding training.

Staff will:

- only publish images of learners where they and their parent/carer have given explicit written consent to do so.
- only take images where the child is happy for them to do so.
- ensure that a senior member of staff is aware that the equipment is being used and for what purpose.
- avoid making images in a one-to-one situation.

Staff will not

- take images of learners for their personal use.
- display or distribute images of learners unless they are sure that they have parental consent to do so (and, where appropriate, consent from the child).
- take images of learners using personal equipment.
- take images of learners in a state of undress or semi-undress or which could be considered as indecent or sexual
- take images of a child's injury, bruising or similar or make audio recordings of a child's disclosure.

14. All members of staff, including volunteers, will ensure that all images are available for scrutiny and will be able to justify any images in their possession.

15. Images will only be retained when there is a clear and agreed purpose for doing so. Vikki Reeves and Hannah Ferris will ensure that all images are permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

16. Images will be stored in an appropriately secure place; on a federation owned device or network.

17. Images in the school/nursery will remain on site, unless prior explicit consent has been given by the DPO and DSL and the parent/carer of any child or young person captured in any images. Should permission be given to take images off site, all relevant details will to be recorded, for example who, what, when and why. Images taken offsite will be kept securely for example with appropriate protection.

18. Any memory stick/storage or device containing images of children to be taken offsite for further work will be suitably protected and will be logged in and out by the DPO and/or DSL; this will be monitored to ensure that it is returned within the expected time scale.

19. The DPO and/or DSL reserve the right to view any images taken and can withdraw or modify a member of staffs' authorisation to take or make images at any time.

20. Any apps, websites or third-party companies used to share, host or access children's images will be risk assessed prior to use.

21 The school/nursery will ensure that images always are held in accordance with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act, and suitable child protection requirements, if necessary, are in place.

22. Images will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies will not to be taken of any images without relevant authority and consent from the DPO and/or DSL and the parent/carer.

Safe Practice when taking images

23. Careful consideration is given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

24. The Lightyear Federation will discuss the use of images with children in an age-appropriate way.

25. A child or young person's right not to be photographed or videoed is to be respected. Images will not be taken of any child or young person against their wishes.

26. Photography or video recording is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.

27. Images or videos that include children will be selected carefully for use, for example only using images of children who are suitably dressed.

Publication and sharing of images

28. Full names of children will not be used on the school/nursery website or other publication, for example newsletters, social media channels, in association with photographs or videos.

29. The school/nursery will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.

30. Where images that could identify staff or children are published online, the school/nursery will ensure any image metadata is removed and lower resolution images are used.

Usage of apps/systems to share images with parents

31. The school/nursery uses Tapestry and Class Dojo to upload and share images of children with parents.

32. The use of the system has been appropriately risk assessed, and the governing body/Executive Headteacher/Head of School has taken steps to ensure all data stored is held in accordance with GDPR and the Data Protection Act.

33. Images uploaded to Tapestry and Class Dojo will only be taken on school/nursery devices.

34. All users of Tapestry and Class Dojo are advised on safety measures to protect all members of the community, for example, using strong passwords, logging out of systems after use etc.

35. Parents/carers will be informed of the expectations regarding safe and appropriate use (For example, not sharing passwords or copying and sharing images) prior to being given access. Failure to comply with this may result in access being removed.

Use of Video Surveillance, including CCTV

36. The Lightyear Federation has a separate CCTV policy which documents expectations and procedures in relation to video surveillance and CCTV.

Use of webcams

37. Parental consent will be obtained before webcams will be used within the setting environment with children.

38. Where webcams are used with children to access or engage with education (for example remote learning), images and recording will be held in accordance with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act, and any necessary child protection requirements will be implemented.

Use of images of children by others

Use of image by parents/carers

39. Parents/carers are permitted to take photographs or video footage of events for private use only.

40. Parents/carers who are using photographic equipment must be mindful of others, including health and safety concerns, when making and taking images.

41. The opportunity for parents/carers to take photographs and/or make videos may be reserved by the federation on health and safety grounds.

42. Parents/carers are only permitted to take or make recording within designated areas of the school/nursery. Photography or filming is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.

43. The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.

44. Parents may contact the federation DPO/DSL to discuss any concerns regarding the use of images.

45. Photos and videos taken by the federation and shared with parents should not be shared elsewhere, for example posted onto social networking sites. To do so may breach intellectual property rights, data protection legislation and importantly may place members of the community at risk of harm.

Use of images by children

46. The school/nursery will discuss and agree age-appropriate acceptable use rules with children regarding the appropriate use of cameras, such as when engaging in remote learning and when onsite. This will include places children cannot take cameras, for example unsupervised areas, toilets etc.

47. The use of personal devices, for example, mobile phones, tablets, digital cameras, is covered within the online safety policy.

48. All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.

49. Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos or videos.

50. Images taken by children for official use will only be taken with parental consent and will be processed in accordance with UK GDPR and the Data Protection Act.

51. Parents/carers will be made aware that children will be taking images of other children and will be informed how these images will be managed. For example, they will be for internal use by the school/nursery only and will not be shared online or via any website or social media tool.

52. Images taken by children for official use will be carefully controlled by the school/nursery and will be checked carefully before sharing online or via digital screens.

Use of images of children by the media

53. Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's, or other relevant media, requirements can be met.

54. Written consent will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (such as first names only) will be published along with images and videos.

55. The identity of any press representative will be verified, and access will only be permitted where the event is planned, and where press are specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.

56. Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the setting is to be considered to have acted in good faith.

Use of external photographers, including videographers and volunteers

57. External photographers who are engaged to record any events officially will be prepared to work according to the terms of our policies, including our safeguarding and child protection policy.

58. External photographers will sign an agreement which ensures compliance with UK GDPR and the Data Protection Act.

59. Images taken by external photographers will only be used for a specific purpose, subject to parental consent.

60. External photographers will not have unsupervised access to children.

Policy breaches

61. Members of the community should report image use concerns regarding image use or policy breaches in line with existing federation policies and procedures. This includes informing the Executive Headteacher/Head of School. Our complaints, safeguarding and child protection, whistleblowing and staff code of conduct has more information in relation to this.

62. Following a policy breach, leadership staff will debrief, identify lessons learnt and implement policy changes as required. Action will be taken in line with existing federation policies and procedures which may include safeguarding and child protection, anti-bullying, online safety and behaviour policies.

63. Advice will be sought, and reports will be made to other organisations in accordance with national and local guidance and requirements. For example, where there may have been a data protection breach, the ICO will be contacted, and if an allegation has been made against a member of staff, contact will be made with the Local Authority Designated Officer (LADO).

Lightyear Federation

Acceptable Use of Technology – Parent/Carer Agreement

As a federation, we are keen to promote safe technology use both in and out of school. We feel that modelling safe technology use and talking about safe behaviours is fundamental in ensuring that your child has the best possible chance of being safe online and reporting concerns appropriately if they do occur. In school we offer regular online safety lessons. We have some statements, documented below, which we feel are important for parents to understand and follow to support their child. If you would like to discuss any of the statements below, please contact the Designated Safeguarding Lead (Hannah Ferris).

1. I will read and discuss the 'Acceptable Use of Technology for Learners' (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I know that my child will be provided with internet access and will use a range of IT systems including computers, laptops, iPads, tablets and other digital devices, the 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 in order to access the curriculum and be prepared for modern life whilst at school.

3. I understand that the AUP applies to my child use of school devices and systems on site and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school or federation.

4. I understand that any use of school devices and systems are appropriately filtered; this means that usage can and will be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. Netsweeper is used as our internet filtering system and is used in addition to physical monitoring and supervision by school staff.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school online safety policy states that my child cannot use personal devices including smart and mobile technology on site. Any child bringing a mobile phone/smart technology to school will be required to switch it off and hand it into the school office or their class teacher at the beginning of the school day. Devices will be returned at the end of the school day.

7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school and federation.

8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

9. I will inform the school or other relevant organisations if I have concerns over my child or other members of the school communities' safety online. I know that I can speak to the Designated Safeguarding Lead (Hannah Ferris), my child's class teacher or a member of the school leadership team if I have any concerns about online safety.

10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

11. I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Visitor and Volunteer Acceptable Use of Technology

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology.

This AUP will help the Lightyear Federation ensure that all visitors and volunteers understand our expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within the Lightyear Federation both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies**.**

2. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the federation ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

3. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material or adult pornography covered by the Obscene Publications Act.

4. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

5. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the federation into disrepute.

Data and Image Use

6. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

7. I understand that I am not allowed to take images or videos of learners unless on a federation device with the class teacher's approval.

Classroom Practice

8. I have read the Safeguarding and Child Protection Policy and am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

9. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

10. I will immediately report any filtering breaches (such as accidental or deliberate access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Hannah Ferris) in line with the federation's safeguarding and child protection policy.

11. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, misuse, plagiarise, or distribute them.

Use of mobile devices and smart technology

12. In line with the federation mobile and smart technology expectations, I understand that mobile phones and personal devices must be switched off/to 'do not disturb', stored securely and can only be used in staff-only areas. If needing to use a mobile phone/personal device, visitors should ask a member of staff who will be able to advise.

Online communication, including the use of social media

13. I will ensure that my online reputation and use of technology is compatible with my role within the federation. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online.
    - I will not discuss or share data or information relating to learners, staff, federation business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the federation code of conduct/behaviour policy and the law.

14. My electronic communication with parents/carers, children and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via federation approved communication channels.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (Hannah Ferris) and/or Executive Headteacher/Head of School.

Policy compliance, breaches or concerns

15. If I have any queries or questions regarding safe and professional practise online either in school/nursery or off site, I will raise them with the Designated Safeguarding Lead (Hannah Ferris) and/or Executive Headteacher/Head of School.

16. I understand that the federation may exercise its right to monitor the use of its devices information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

17. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Leads (Hannah Ferris) in line with the federation safeguarding and child protection policy.

18. I will report concerns about the welfare, safety, or behaviour of staff to the Executive Headteacher/Head of School, in line with the allegations against staff policy.

19. I understand that if the federation believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the federation may invoke its disciplinary procedures.

20. I understand that if the federation suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the Lightyear Federation visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……

Signed: ……

Date (DDMMYY)……..

Lightyear Federation Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguard all members of the school community when taking part in remote learning, for example during any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Microsoft Teams, Zoom or Google Classrooms
    - These systems have been assessed and approved by the ICT technician and Executive Head Teacher.

2. Staff will only use federation managed or specific, approved professional accounts with learners and/or parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.

3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT without prior consent:
    - Monday to Friday between 08:00 and 17:00

4. All remote lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.

5. Live streamed remote/online learning sessions will only be held with approval and agreement from the Senior Leadership Team.

Data Protection and Security

6. Any personal data used by staff and captured by the online learning platforms when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

7. All remote learning and any other online communication will take place in line with current federation confidentiality expectations and will not be shared unless necessary and with the appropriate person.

8. All participants will be made aware that online platforms can record activity and if the content is being recorded. Consent from those involved in the session is required if settings are recording activity.

9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

10. Only members of the Lightyear Federation community will be given access to the online learning platform login details and passwords.

11. Access to the online learning systems will be managed in line with current IT security expectations as outlined in the AUP and Online Safety Policy. e.g the use of strong passwords, not sharing passwords, logging off when not in use and locking screen when not with the device.

Session Management

12. Staff will record the length, time, date, and attendance of any sessions held. This will be recorded on sheets disseminated by the DSL in the event of a lockdown.

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Not allowing children to share screens, staff being aware of how to mute children, keeping meeting ID's private, disabling chat where appropriate.

14. When live streaming with learners:
    - contact will be made via learners' school provided email accounts or logins
    - staff will mute/disable learners' videos and microphones as appropriate in line with the session being taught and age of the children.
    - at least 2 members of staff will be present. If this is not possible, SLT approval will be sought.

15. Live 1 to 1 session will only take place with approval from a member of SLT.

16. A pre-agreed invitation/email (as relevant to system being used) detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

17. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

19. All participants are expected to behave in line with existing school policies and expectations. This includes, but is not limited to;
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
    - Recordings of learning should not be sent without the knowledge of Senior Leadership Team

20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

21. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
    - Ensure that family are not visible in the background
    - Behave professionally and model safe internet behaviour.

22. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

23. Participants are encouraged to report concerns during remote and/or live streamed sessions:

24. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to Hannah Ferris DSL/SPD.

25. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

26. Sanctions for deliberate misuse may include: restricting/removing use of online learning, contacting parents or contacting police if a criminal offence has been committed.

27. Any safeguarding concerns will be reported to Hannah Ferris, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Lightyear Federation Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……

Date…….