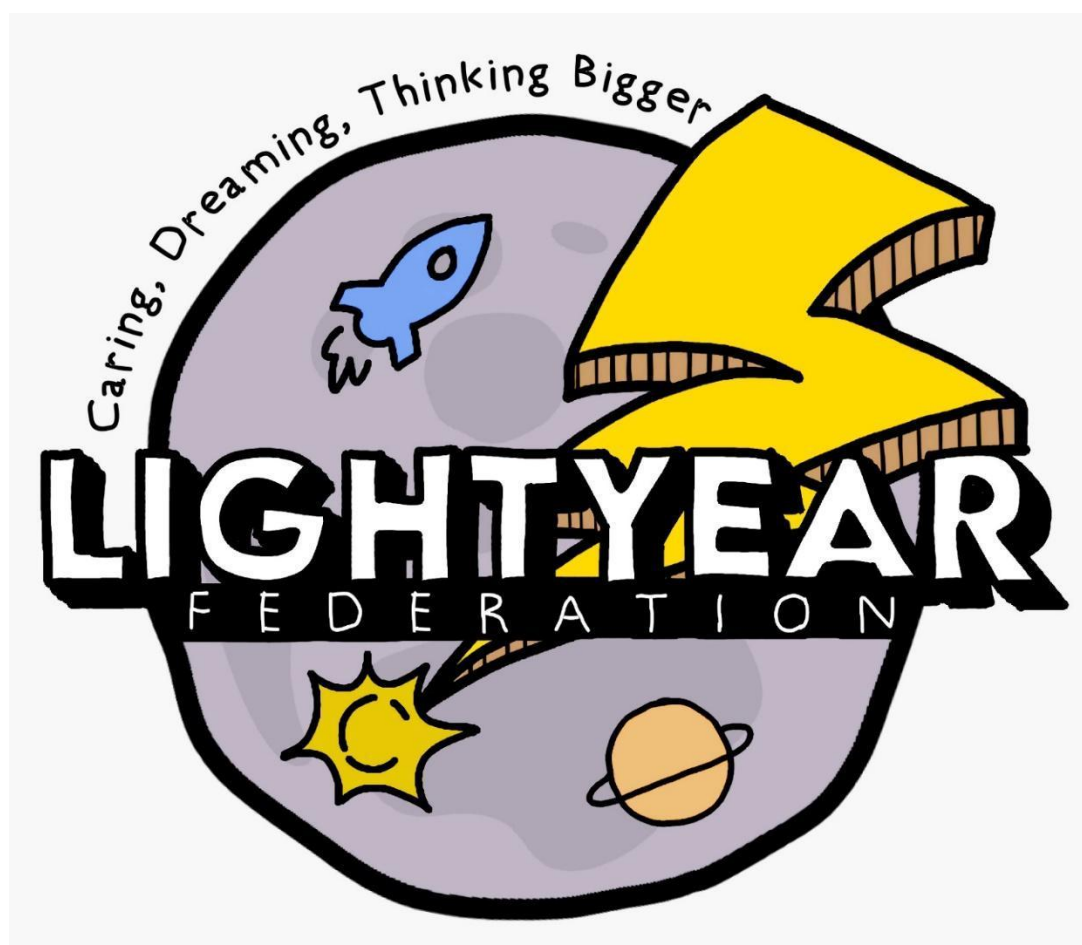




Acceptable Use of Technology and Image Use Policy September 2026

Policy lead	Hannah Ferris
Date approved by Governing Body	
Review date	September 2027 – or following any updates to national and local guidance and procedures.

Contents:

Pupil Acceptable Use of Technology	3
Early Years and Key Stage 1 (0-6)	3
Key Stage 2 (7-11)	3
Pupils with Special Educational Needs and Disabilities (SEND)	5
Acceptable Use of Technology	7
The Lightyear Federation Parent/Carer AUP Acknowledgement Form	7
Staff Acceptable Use of Technology Policy (AUP)	9
Visitor/Volunteer Acceptable Use of Technology Policy	16
Wi-Fi Acceptable Use Policy	20
Remote/Online Learning AUP - Staff Statements	22
Image Use Policy	25

The copyright of these materials is held by Kent County Council. Educational settings are granted permission to use, reproduce and adapt all or part of the materials for their own not-for-profit purposes, provided that Kent County Council's copyright is acknowledged and the materials are not sold, distributed commercially or presented as the intellectual property of another organisation.

Pupil Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when a grown-up is with me.
- I check with a grown-up before I click on links or things online.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school accounts, computers and tablets, including if I use my school accounts at home.
- 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 school rules, my parents/carers will be told and I may not be able to use the computers at school.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

Key Stage 2 (7-11)

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 in school.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if I know what they do, or I will ask a safe adult first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- If someone online asks to meet me, I will tell a safe adult straight away.

Learning

- I follow the school rules about mobile phones and smart technology. If I bring a mobile phone or smart device to school, I will not use it during the school day. 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/or search engines that a teacher has chosen or given me permission to use.
- I use school devices for school work, unless I have been told otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

True

- I know that some things or people online might not be honest or truthful.
- If I'm unsure if something online is true, I will check other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when my teacher says it is allowed.
- I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- 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 know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidentally come across any of these, I should report it to a teacher or adult in school, or a parent or carer at home.
- 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

- If I see anything online that makes me feel worried, upset, or frightened, I will lock the screen and tell an adult straight away.
- If I am aware of anyone being unkind or unsafe with technology, I will report it to an adult at school.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I understand that the adults at school are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

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 checked/monitored to help keep me safe, even if I use them at home. This means someone at the school can see and check my online activity when I use school devices and networks if they are worried about my or anyone else's safety or behaviour.
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the school rules then my parents/carers will be told and I may not be able to use the computers at school.

Pupils with Special Educational Needs and Disabilities (SEND)

Pupils with SEND functioning at Levels P4 –P7

- I only use phones, tablets or computers when a grown-up says it is okay.
- I make good choices on the computer.
- I use kind words on the internet.
- I tell a grown-up if I see or hear something online that upsets me.
- I know that if I do not follow the school rules then I may not be able to use technology in school.

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

- I ask a grown-up if I want to use a phone, tablet or computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then I may not be able to use technology in school.
- I tell a grown-up if I want to talk to someone 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 online that worries me, I will tell a grown-up.

Pupils 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 use phones, tablets or computers when an adult says it is okay.
- I keep my information private on the internet.
- I ask an adult before I take or share a photo, video or message.
- I know that if I do not follow the school rules then I may not be able to use technology in school.
- I tell an adult if I want to talk to people on the internet.
- If I want to meet someone online, I talk to an adult.
- 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 worries or upsets me, I will tell a teacher.

Artificial intelligence for children with SEND

- AI means technology that can make or suggest things, like words, pictures, videos, voices, answers or ideas. I will only use AI when an adult says I can.
- I use AI with help from an adult.
- I ask an adult before I use AI.

- I will only use AI tools that the school has said I can use.
- I will only use AI tools in the way staff have shown me.
- I do not put information about me into AI.
- I do not put information about other people into AI.
- I will not put names, photos, personal information or private information about me or other people into AI tools.
- I do not use AI to pretend to be someone else.
- I do not use AI to make fake pictures, voices, videos or messages about people.
- I do not use AI to make anything unkind or upsetting about another person.
- I know that AI can make mistakes, so I will check information with an adult.
- If AI shows me something worrying, unsafe, unkind or confusing, I will stop and tell an adult.
- I understand that AI can help me learn, but it should not do all my work for me.
- I will ask for help if I am not sure whether I can use AI for my work.

Wider safe technology use for children with SEND

- I ask an adult before I use technology.
- I use technology in the way adults have agreed.
- I follow the school rules for phones, devices, cameras, computers and AI tools.
- I tell an adult if something online or on a device makes me worried.
- I do not use technology to upset, trick or hurt other people.
- I ask an adult before I share information, pictures or videos.
- I know adults at school can help me use technology safely.

Acceptable Use of Technology

The Lightyear Federation Parent/Carer AUP Acknowledgement Form

1. I have received and read The Lightyear Federation Pupil Acceptable Use of Technology Policy (AUP) and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.
2. I understand that my child will be provided with internet access and may use a range of technology, devices, accounts and online services at school to support their learning, development and preparation for life in a digital world.
3. I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using:
 - school-provided devices, accounts, systems and internet access;
 - school-provided technology away from the setting;
 - personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the school, or raises a safeguarding or behaviour concern.
4. I understand that my child will receive age and ability-appropriate online safety education to help them use technology safely and responsibly, both within and outside the school. I recognise that education, appropriate supervision, open communication and opportunities to seek help remain important alongside technical measures such as filtering and monitoring.
5. I understand that access to online content through school devices and systems is appropriately filtered and that use of school-provided devices, accounts and systems may be monitored, including when they are used away from the setting. I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk.
6. I understand that access to online content through school-provided devices, systems and internet services is appropriately filtered. The Lightyear Federation's education internet connectivity is provided through Broadband 4 (Part of PSD Group) and uses [Netsweeper](#) as the filtering system to block access to harmful content. Netsweeper blocks internet access to illegal content and activity as identified in the Online Safety Act and is a member of Internet Watch Foundation (IWF).
7. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements. I am aware that my child's use of school-provided devices, accounts and systems may be monitored, including when those accounts or systems are used away from the school. This is achieved through:
 - physical monitoring/supervision by staff while children are using technology;
 - computing areas set up so that computers can be observed and monitored by staff moving around the room;
 - monitoring internet and web access through a daily review of the logfile information.
8. I am aware of the school's expectations concerning mobile phones and smart devices and will support my child to follow them. If my child may need an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will support any individual arrangements agreed for my child. If I need to contact my child

during the school day, I will use the school office or another agreed contact route, unless an alternative arrangement has been agreed.

9. I will support my child to understand and follow the school's expectations for safe, kind, lawful and responsible technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.
10. I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the community.
11. If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered. Further details are available on the school website.
12. I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include the class teacher, a member of the safeguarding team, or headteacher. Where necessary, I may also report the concern to another relevant organisation.
13. If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so. I understand that there may be circumstances in which the setting must first follow its safeguarding procedures or seek advice from another agency. Where behaviour may be unlawful or presents a risk to safety, the school may seek appropriate safeguarding, police or legal advice.
14. I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home. I will help my child understand how and where to seek support.
15. Where my child accesses remote or online learning, I will support them to follow the school's remote/online learning expectations. I will help my child to access learning from an appropriate location and provide supervision and support that reflects their age, understanding and needs. I understand that the school will provide information about the systems and sites my child is expected to access and who from the school, if anyone, they will interact with online.
16. I know that I can seek online safety information or support from the school by contacting Hannah Ferris, Designated Safeguarding Lead (spd@lightyear.kent.sch.uk).

I confirm that I have read and understood The Lightyear Federation Pupil Acceptable Use of Technology Policy and have discussed its expectations with my child. I agree to support its expectations and the safe, lawful and responsible use of technology by my child.

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out The Lightyear Federation's expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect pupils, staff, systems and the wider school/nursery community from accidental or deliberate misuse.

All staff are asked to sign a staff compliance sheet to confirm that they have read and understood this AUP.

Policy scope

1. I understand that this policy applies to my use of technology systems and services provided by the school/nursery or accessed by me as part of my role within The Lightyear Federation, both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the school/nursery community, uses school/nursery systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school/nursery.
2. I understand that The Lightyear Federation Acceptable Use of Technology Policy (AUP) should be read and followed in line with The Lightyear Federation safeguarding and child protection policy and staff code of conduct.
3. I am aware that all staff should ensure that their technology use is consistent with the school/nursery ethos, federation staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of The Lightyear Federation devices and systems

4. I will use federation-provided or approved equipment, systems and internet services when working with pupils, unless otherwise formally agreed by the headteacher.
5. I understand that school/nursery equipment, systems and internet services are provided for education and/or professional use. Reasonable personal use is permitted and, where allowed, must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.
6. Where I deliver or support remote/online learning, I will comply with The Lightyear Federation remote/online 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 follow the federation's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.

- 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 take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to NCS Technology.
9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Technician.
10. I will ensure that any personal data is kept in accordance with data protection legislation and 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 site, such as via email, will be suitably protected. This may include data being encrypted by a method approved by the federation.
 - I will only process or share personal data through federation-approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.
11. I will not keep documents which contain federation/school/nursery 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 school/nursery learning platform to upload any work documents and files in a password-protected environment or federation-provided VPN.
12. I will not store any personal information on the school/nursery IT system, including school laptops or similar devices issued to members of staff, that is unrelated to school/nursery 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 Lightyear 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 Support Provider as soon as possible via helpdesk@ncstechnology.co.uk.
16. If I have lost any school/nursery/federation related documents or files, I will report this to the ICT Support Provider, NCS Technology and The Lightyear Federation Data Protection Officer as soon as possible.
17. I will follow the federation image use policy when taking, using, storing or sharing images or recordings of pupils. Images and recordings must always be appropriate and must only be taken using

school/nursery-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of pupils. Images and recordings will only be taken, used or shared in line with the federation image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

18. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant federation policies.
19. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider, in line with the federation safeguarding and child protection policy.
20. I will follow federation expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools.
21. I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.
22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school/nursery community. However, I 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, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
 - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
 - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of pupils, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the DPO/leadership team has confirmed that the processing is lawful and appropriate.
 - I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
 - I will not use AI to make decisions about pupils, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
 - Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.

- I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the federation safeguarding and child protection, behaviour, anti-bullying, staff conduct and data protection procedures.
23. I will promote online safety with the pupils 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 pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble or being judged for talking about something which happened to them online.
 - involving the DSL or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils 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.
 - making informed decisions to ensure any online safety resources used with pupils are appropriate.
24. 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 phones and smart devices

25. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff behaviour policy/code of conduct, mobile phone policy and the law. I am responsible for:
- Ensuring that my personal devices are configured appropriately; this includes disabling notifications, image display, recording and sharing functions where these could compromise safeguarding, professional boundaries or the learning environment. Where devices cannot be configured to meet these expectations, they must not be worn.
 - Keeping personal mobile and smart devices in a safe and secure place during teaching, learning or supervision time, for example, in a drawer or in staff member's pigeon hole (with the exception of using a personal mobile phone or smart devices for authenticating an account, devices should not be used during teaching, learning or supervision periods, unless permission has been given in advance by the senior leadership team, for example, in emergency circumstances).
 - Ensuring my personal mobile and smart devices are switched off or set to 'silent' or 'do not disturb' modes during teaching sessions and other times when supervising pupils.
 - Securing, disabling or hiding Bluetooth, 'AirDrop' or similar sharing and communication functions during teaching and learning sessions or when supervising pupils.
 - Ensuring that any content brought onto site via personal mobile or smart devices is appropriate to my professional role and consistent with behaviour and safeguarding expectations.
26. I will model safe and professional use of mobile phones and smart devices and will support the school/nursery's expectations for pupils.

27. Where devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school provided devices where available. Staff are permitted to use their personal devices for authentication purposes.
28. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

29. I will ensure that my use of communication technology, including social media, is compatible with my professional role, does not interfere with my work duties, and takes place in line with the child protection policy, staff code of conduct, social media policy and the law.
30. I will protect myself, my professional reputation and the reputation of the federation/school/nursery online. I will not discuss or share data or information relating to pupils, staff, federation/school/nursery business or parents/carers on social media.
31. My electronic communications with current and former pupils 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-provided communication channels and systems, such as a federation email address, user account or telephone number.
 - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with pupils or their families, unless this has been formally approved, risk assessed and recorded by leaders.
 - I will not share any personal contact information or details with pupils, such as my personal address, email address or phone number.
 - I will not share personal information about my private life with pupils online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.
 - I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former pupils, or their parents/carers, where this is linked to my role, the school/nursery or could blur professional boundaries. Any attempted contact will be reported to the DSL and/or headteacher.
 - Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or headteacher. This is to help safeguard pupils, staff and the wider community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
 - Where digital communication with pupils or families is required, I will follow the federation's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

32. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
33. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using federation systems, school/nursery devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on federation premises, during working time, or in any context linked to my role.
34. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.
35. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the federation safeguarding and child protection policy.
36. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the headteacher, in line with the federation safeguarding and child protection policy, staff code of conduct and allegations against staff policy.

Policy compliance and breaches

37. If I have any queries or questions regarding safe and professional practice online, either in school/nursery or off site, I will raise them with the DSL and/or the headteacher.
38. I understand that The Lightyear Federation may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of pupils and staff.
 - This includes monitoring all school/nursery-provided devices and school/nursery systems and networks including school/nursery-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school/nursery-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.
 - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.
39. I understand that if the federation believes that unauthorised and/or inappropriate use of school/nursery devices, systems or networks is taking place, the federation may invoke its disciplinary procedures as outlined in the staff code of conduct.
40. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL/headteacher so it can be recorded and managed transparently.

41. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
42. I understand that if the federation believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.
43. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the data protection officer will be informed promptly so that any data protection, information governance or reporting requirements can be considered.
44. I understand that if the federation suspects criminal offences have occurred, the police will be informed where appropriate.
45. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher before taking action. I will act in a way that safeguards pupils, protects professional boundaries, and is open to scrutiny.

Visitor/Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that visitors and volunteers understand our expectations for safe, lawful and responsible technology use while on site, when using The Lightyear Federation systems, or when acting in a role connected to The Lightyear Federation. This AUP helps The Lightyear Federation explain expectations around safeguarding, professional conduct, data protection, image use, mobile phones, online communication and reporting concerns.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems, services, devices or information provided by The Lightyear Federation, or accessed by me as part of my role, visit or activity with Greatstone Primary School and Nursery, or Repton Manor Primary School. It also applies to personal devices or accounts where their use takes place on site, involves The Lightyear Federation community, is linked to my role or visit, or could affect safeguarding, confidentiality, data protection, professional boundaries or the reputation of The Lightyear Federation, Greatstone Primary School and Nursery, or Repton Manor Primary School.
2. I understand that this AUP should be read and followed in line with relevant federation, school and nursery policies, including the staff code of conduct, child protection policy, visitor/volunteer procedures, image use policy and mobile phone/smart device policy.
3. 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 school/nursery ethos, federation staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download or access any materials which are illegal, including but not limited to child sexual abuse material, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
5. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using federation systems, school/nursery devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces, where this takes place on school/nursery premises, during my visit/volunteering activity, or in any context linked to my role.
6. I will not engage in any online activity, digital communication or behaviour that could compromise safeguarding, professional boundaries or the reputation of the federation/school/nursery.

Data and image use

7. Where I have access to personal data, confidential information, safeguarding information, school/nursery systems, records or devices, I will only access, use or share this information where it is necessary for my agreed role, visit or activity and in line with data protection legislation and federation procedures. I will not copy, download, photograph, record, forward or share information unless this has been authorised.

8. I will not take, use, store or share images or recordings of pupils during lessons, visits, trips, events, performances, activities or celebrations unless this has been specifically authorised by the school/nursery and is in line with the federation image use policy. Where authorised, images or recordings must only be taken, used, stored or shared using school/nursery approved equipment, accounts and systems, unless leaders have made a specific, risk-assessed decision otherwise. I will not take images or recordings of pupils for personal use or share them on personal devices, personal accounts, social media, messaging apps or online groups.

Classroom practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils. Children should always be supervised when accessing technology and should only do so with permission from a staff member.
10. Where I am supporting pupils, I will reinforce safe and appropriate technology use and will follow staff instructions and federation policies.
11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the federation community, I will report this to a Designated Safeguarding Lead (DSL) and IT Technician in line with federation safeguarding and child protection policy.
12. 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.
13. I will not record, transcribe, livestream, use AI note-taking tools, recording bots or automated meeting summary tools during any meeting, visit, lesson, activity or professional discussion unless this has been specifically authorised by the federation and is in line with safeguarding, confidentiality, consent and data protection expectations.

Use of mobile phones and smart devices

14. In line with the federation mobile phone and smart device policy, I will model safe and appropriate use of mobile phones and smart devices while on site. I will not use my own mobile phone or smart device in front of pupils unless this has been agreed by the school/nursery leadership team and is directly linked to my role, visit or volunteering activity. I will follow the federation's expectations about where and when mobile phones and smart devices may be used or stored.

Online communication, including the use of social media

15. I will ensure that my online conduct, reputation and use of technology are compatible with my role within the school/nursery. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.

16. Any electronic communication with pupils, parents/carers or staff as part of my role, visit or volunteering activity will take place within clear professional boundaries and be transparent and open to scrutiny.
- Communication will take place using federation approved channels, such as a federation-provided email address, account, platform or telephone number.
 - I will not use personal devices, personal email, personal social media, private messaging apps, gaming accounts or personal phone numbers to contact pupils or their families.
 - Any pre-existing relationships, links or situations that may affect how I apply this AUP will be discussed with the DSL and/or headteacher.
17. I will respect confidentiality and will not post, comment on, discuss or share information online about pupils, staff, families, incidents, activities or anything I become aware of through my role, visit or volunteering activity. This includes comments, images, videos, recordings or information shared on personal social media, messaging apps, online groups or community forums.

Policy compliance, breaches or concerns

18. If I have any queries or questions regarding safe and professional practice online either in school/nursery or off site, I will raise them with the Designated Safeguarding Lead, Hannah Ferris, and/or the headteacher.
19. I understand that the federation may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of pupils and staff.
- This includes monitoring all school/nursery-provided devices and school/nursery 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.
20. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL, in line with the federation safeguarding and child protection policy.
21. I will report concerns about the welfare, safety, conduct or behaviour of staff, including online, digital, device-related, image-related or technology-linked concerns, to the headteacher, in line with the federation safeguarding and child protection policy, staff code of conduct, and/or allegations against staff policy.
22. I understand that if the federation believes that illegal, unauthorised or inappropriate use, unacceptable behaviour, or a breach of this AUP has taken place, action may be taken in line with relevant safeguarding, behaviour, complaints, volunteer, contractor, visitor, data protection, low-level concerns or allegations procedures, as appropriate. This may include ending or restricting access to the site, systems or activities, informing an employer/agency/organisation, seeking advice from the LADO, informing the data protection officer, or contacting the police where appropriate.
23. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the DSL/headteacher without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

24. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the Data Protection Officer (DPO) will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

25. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher.

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).....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school/nursery Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the federation ethos, relevant policies and the law.

1. The federation provides Wi-Fi for education use. Users may seek permission to connect personal devices to the school/nursery Wi-Fi and this will be considered on a case-by-case basis.
2. Use of the Wi-Fi falls under The Lightyear Federation Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All pupils, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.
3. The Lightyear Federation reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.
4. The Lightyear Federation-owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.
5. I will take reasonable steps to ensure that any personal device connected to school/nursery Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.
6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school/nursery security, filtering or monitoring systems, or download unauthorised software, applications or files.
7. I will not use school/nursery Wi-Fi to access, create or share illegal or harmful content, compromise another person's safety or privacy, interfere with systems, or breach relevant federation policies.
8. I will not use school/nursery Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with federation data protection and safeguarding procedures.
9. Staff using school/nursery Wi-Fi on personal devices remain subject to the staff code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.
10. The Lightyear Federation takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school/nursery Wi-Fi, users do so at their own

discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.

11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Lead or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL, identified technical contact or headteacher.
12. I understand that activity carried out through school/nursery Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that The Lightyear Federation can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
13. If The Lightyear Federation suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant federation procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher, LADO or police.

**I have read, understood and agreed to comply with The Lightyear Federation Wi-Fi
Acceptable Use Policy.**

NameSignedDate (DDMMYY).....

Remote/Online Learning AUP - Staff Statements

The Lightyear Federation Staff Remote/Online Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguard all members of The Lightyear Federation 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 headteacher.
2. Staff will only use federation-managed or specifically approved professional accounts with pupils and/or parents/carers.
 - Use of any personal accounts to communicate with pupils 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 federation-provided equipment where possible e.g. a school laptop, tablet, or other mobile device.
3. Online contact with pupils 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 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. Participants will be informed about any activity that records or retains information such as attendance, chat messages, shared files, audio or video recordings, and how this information will be used.
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. 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 electronic sheets disseminated by the DSL in the event of school closure.
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 IDs private, disabling chat where appropriate.
14. When live streaming with pupils:
- contact will be made via pupils' school provided email accounts or logins
 - staff will mute/disable pupils' 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 one to one 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 pupils/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
 - Pupils 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.
 - Staff will explain any expectations about the location from which pupils take part. These will reflect their age, needs, privacy, home circumstances and the nature of the session.
17. Alternative approaches/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 the 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 members 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.

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.

The Lightyear Federation 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 curricula 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 and limited to what is necessary 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 Officers (DPO) within The Lightyear Federation 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 federation. 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 pupils 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 pupils for their personal use.
- display or distribute images of pupils unless they are sure that they have parental consent to do so (and, where appropriate, consent from the child).
- take images of pupils using personal equipment.
- take images of pupils 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. Images should be 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 headteacher/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 headteacher/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 staff's 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 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 rooms, 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 these systems has been appropriately risk assessed, and the governing body/headteacher 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 are used within the school/nursery environment with children.

38. Where webcams are used with children to access or engage with education (for example remote learning), images and recordings 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 images 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 recordings within designated areas of the school/nursery. Photography or filming is not permitted in sensitive areas such as changing rooms, 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 unless a DBS certificate check has taken place.

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 to the headteacher/DSL. 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).