Acceptable Use of Technology Policy
September 2024

Policy lead	Hannah Ferris
Date approved by Governing Body	Draft - To be Ratified
Date uploaded to website	October 2024
Review date	September 2025 – or following any updates to national and local guidance and procedures.

Contents

Acceptable Use Policy for Learners

Acceptable Use of Technology Statements.

Early Years and Key Stage 1

- I understand that this Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and devices.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I know that if I do not follow the rules, my parents/carers will be informed and internet privileges will be removed.
- I have read and talked about these rules 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 behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult. I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.

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 phone while I am at school or on school trips.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.

Trust
- I know that not everything or everyone online is honest or truthful.
- I will check content on various sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them with anyone and 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 check before I download software or data from the internet.
- 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 a an adult in school, or a parent or carer at home.
- If I see anything online that I should not or that makes me feel worried or upset, I will lock the screen and tell an adult straight away.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.

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 devices and systems are monitored to help keep me safe, including if I use them at home. This means someone at the school may be able to see and check my online activity when I use school devices and networks if they are concerned about my or

anyone else's safety or behaviour.
- I have read and talked about these rules with 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. However, 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.
- If I 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 I do not like, I will tell a grown-up.

Lightyear Federation Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, 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 with other members of the school community or when accessing school systems.

Name…… Signed……..…..

Class…….…… Date…….

Parent/Carer's Signature…….…….

Date……

Parent/Carer Acceptable Use of Technology

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 and the school. If you do not agree with any of the statements below, please contact the Designated Safeguarding Lead (Hannah Ferris).

1. I have read and discussed The Lightyear Federation Acceptable Use of Technology Policy (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, tablets and other digital devices, Internet (which may include search engines and educational websites), learning platforms, remote learning platform/tools and intranet, email, digital cameras, web cams and video cameras 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.

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.

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 hand this 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 add any images, video, sounds or text 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.

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's 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.

I have read, understood and agree to comply with the Lightyear Federation Parent/Carer Acceptable Use of Technology Policy.

Child's Name…… Child's Signature ……

Class……..……Date……

Parent/Carer's Name…….....

Parent/Carer's Signature……...

Date…….

Acceptable Use of Technology for Staff

Staff Acceptable Use of Technology Policy

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 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 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 behaviour 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 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.

6. Where I deliver or support remote learning, I will comply with the school 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 school systems and will not disclose my password or security information to others. A strong password has numbers, letters and symbols, 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 IT 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 school. ***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 IT technician as soon as possible.

16. If I have lost any federation related documents or files, I will report this to the IT Technician and school 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 school 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.

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/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 the use of AI as part of our education/curriculum approaches is only permitted by staff where the following have been satisfied;

- A risk assessment has been undertaken, and written approval has 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 or assessments).
- 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.

22. I will promote online safety with the learners 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 school email address, user account or 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 schools 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 Exec Head Teacher***.***

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 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.

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

Name of staff member: ……

Signed: …….....

Date (DDMMYY)……...

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 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, systems 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.

I have read, understood and agreed to comply with the Lightyear Federation WIFI Acceptable Use Policy

Staff Member Name: ……

Date…….

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 school device with the class teacher's approval.

Classroom Practice

8. I 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 access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Hannah Ferris) in line with the school 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. I have read and understood the federation online safety policy which covers expectations regarding staff and learners' use of mobile technology and social media.

13. I will ensure that my use of mobile devices and smart technology is compatible with my role and takes place in line with the federation online safety police and the law.

14. 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.

15. Any communication with parents/carers, children and professionals will be face to face and will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - 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 this will be discussed with the DSL (Hannah Ferris) and/or Executive Headteacher/Head of School.

Policy compliance, breaches or concerns

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

17. I understand that the school may exercise its right to monitor the use of federation 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.

18. 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.

19. 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.

20. 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.

21. 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…….