Acceptable Use of Technology Policy
March 2023

Policy lead	Hannah Ferris
Date approved by Governing Body	
Governor signature	
Review date	January 2024

Contents

Acceptable Use Policy for Learners

Acceptable Use of Technology Statements.

Early Years and Key Stage 1 (0-6 years old)

I understand that the 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.
• 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, including when I am at home.
• I always tell an adult if something online makes me feel upset, unhappy, or worried.
• I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
• I know that if I do not follow the rules, internet privileges will be removed.
• I have read and talked about these rules with my parents/carers.

Key Stage 2 (7-11years old)

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.

Learning

• 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.
• If I need to learn online at home, I will follow the remote learning AUP.

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. 4 Acceptable Use Policy
• I always credit the person or source that created any work, images, or text I use.

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.

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 when I use them at home.
• I have read and talked about these rules with my parents/carers.
• I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
• I know that if I do not follow the school rules then internet privileges will be removed.

Tell

• If I see anything online that I should not or that makes me feel worried or upset, I shut the laptop lid or turn off the screen and tell an adult straight away.
• 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 bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.
• I know that I am not allowed on personal email, social networking sites or instant messaging in school.
• If, for any reason, I need to bring a personal/smart device and/or mobile phone into school, I know that it is to be handed in to my class teacher or the office and then collected at the end of the school day.
• I know that all school devices/computers and systems are monitored, including when I am using them at home.
• I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Learners use of mobile and smart technology

Parents should discourage pupils from bringing mobile phones/devices to school on the grounds that they are valuable and could be lost or damaged. However, we recognise that for older children, mobile phones may have a part to play in securing pupils' personal safety before and after school and on journeys to and from school.
If a pupil needs to contact his/her parents/guardians they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly.
Under no circumstances will pupils be allowed to take mobile phones on school excursions.
The school accepts no responsibility for any loss or damage whilst the device is on school premises.

Procedures

• Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
• Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies.
• Mobile phones and personal devices must not be taken into classrooms, educational visits or residential trips. They must be handed into the school office. The phone/device must be switched off when entering the school ground and only switched back on again when leaving the school grounds. Learners found in possession of a mobile phone will have it confiscated and their parent/carer will be asked to collect it at the end of the day.
• Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour. Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy. Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies. Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers at the end of the day. Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate. Where there is a concern that a child is at risk of harm, we will contact respond in line with our child protection policy. If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP). I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.

2. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.

Name: ……

Signed: …….....

Date (DDMMYY)……...

Parent/carers name: ……

Parent/Carer Signature: …….....

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 school 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 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 and online and offline 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 school staff behaviour policy/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 school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, 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.
    - I will protect the devices in my care from unapproved access or theft.

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 them 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 school 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 school 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.***

11. I will not keep documents which contain school 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 learning platform to upload any work documents and files.

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

13. I will ensure that school 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 school.

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 (Simon Rogers) as soon as possible.

16. If I have lost any school related documents or files, I will report this to the IT Technician (Simon Rogers) 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 consent.

Classroom Practice

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in insert names of relevant policies e.g. child protection, online safety, remote learning AUP.

19. I have read and understood the school mobile technology and social media policies.

20. 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.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Use of Social Media and Mobile Technology

23. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media.

24. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy/code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the social media policy.
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the mobile technology policy.
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school behaviour policy/code of conduct and the law.

25. 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 school 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 Head Teacher.

26. 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 DSL.

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

28. 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.

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

Policy Compliance

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

Policy Breaches or Concerns

31. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school child protection policy.

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

33. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures.

34. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures.

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

I have read, understood and agreed to comply with Lightyear Federation School 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)……..

Lightyear Federation 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, with my child, have read and discussed the Lightyear Federation learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.
3. I am aware that any use of school devices and systems may 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.
4. I am aware that the school mobile technology policy states that my child cannot use personal device and mobile technology on site.
5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.
6. 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.
7. 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.
8. 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.
9. 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.
10. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Visitor and Volunteer Acceptable Use of Technology

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

This AUP will help the Lightyear Federation ensure that all visitors and volunteers understand the school's 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 school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

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

4. I understand that I am not allowed to take images or videos of learners unless on a school device with the class teachers approval.

Classroom Practice

5. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

6. 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.

7. 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 child protection policy.

8. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Social Media and Mobile Technology

9. I will ensure that my online reputation and use of technology and is compatible with my role within the school. 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, school 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 school code of conduct/behaviour policy and the law.

10. 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 Head of School.

11. 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 Head of School.

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

13. 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.

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

Policy Compliance, Breaches or Concerns

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

16. 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 school child protection policy.

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

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

19. I understand that if the school 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 safeguarding all members of the school community when taking part in remote learning 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 Head Teacher.
2. Staff will only use school 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 a 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 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 school 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 if the content is being recorded. Consent from those involved in the session is required if settings are recording activity. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing data protection policy.
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 school communities will be given access to the online learning platform login details and passwords.
11. Access to the online learning system will be managed in line with current IT security expectations. E.g the use of strong passwords, not sharing passwords, logging off when not in use, locking screen when not with the device. as outlined in policy name.

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 sessions 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 relevant to system being used.
    - Learners and/or parents/carers should not forward or share access links.
    - 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…….

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements

when using any school 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 school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. If the school provides Wi-Fi for the school community, access is for the education use only.

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

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 school 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. School 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 school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. Any school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school 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 school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school 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 school 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 school security and filtering systems or download any unauthorised software or applications.

11.My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school 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 school 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 Head of School or DSL.

15.I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school 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 acceptable Use Policy.

I have read and understood the Lightyear Federation Wifi Use Policy

Staff Member Name: ……..…….

Date…….