The right support, at the right time

Online Safety Policy

Author	**Mrs Emma Rennie-Gibbons**
Policy Adopted	**June 2025**
Policy Published	**June 2025**
Reviewed	**Sept 2026**
Next Review Date	**Sept 2027**

This policy sets out the procedures and responsibilities for Online Safety at the Leading Futures Alternative Provision.

Contents

1.Aims

2. Legislation and Guidance

3. Roles and Responsibilities

4. Educating Learners About Online Safety

5. Educating Parents/ Carers About Online Safety

6. Cyber-bullying

7. Acceptable Use of the Internet in Provision

8. Learners Using Mobile Devices in Provision

9. Staff Using Work Devices Outside Provision

10. How the Provision Will Respond to Issues of Misuse

11. Training

12. Monitoring Arrangements

13. Links With Other Policies

Appendix 1: KS3 and KS4 acceptable use agreement (Learners and Parents/ Carers)

Appendix 2: Acceptable Use Agreement (Staff, Directors, Volunteers and Visitors)

Appendix 3: Online Safety Training Needs – Self-audit For Staff

Appendix 4: Online Safety Incident Report Log

1. Aims

Our provision aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and Directors
- Identify and support groups of learners that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole provision community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for provisions on:

- Teaching online safety in provisionshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and provision staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so.

This policy also reflects the principles of the Online Safety Act 2023, which places duties on technology companies to protect children from harmful online content and strengthens safeguarding arrangements relating to online activity.

3. Roles and Responsibilities

3.1 The Directors

The Directors have overall responsibility for monitoring this policy and holding the whole staff to account for its implementation.

The Directors will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Directors will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Directors will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Directors should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Directors must ensure the provision has appropriate filtering and monitoring systems in place on provision devices and provision networks and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with staff and service providers what needs to be done to support the provision in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Director who oversees online safety is Emma Rennie-Gibbons (DSL).

All Directors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the provision's ICT systems and the internet (Appendix 2).
- Ensure that staff understand this policy, and that it is being implemented consistently throughout the provision.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-provision approach to safeguarding and related policies and/ or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some learners with special educational needs and/ or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.3 The Designated Safeguarding Lead (DSL)

Details of the provision's Designated Safeguarding Lead (DSL) are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in provision, in particular:

- Supporting other Directors in ensuring that staff understand this policy and that it is being implemented consistently throughout the provision.
- Working with the other Director to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on provision devices and provision networks.
- Providing all stakeholders assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the service provider to make sure the appropriate systems and processes are in place
- Working with the other Director, service provider and other staff, as necessary, to address any online safety issues or incidents.

- Managing all online safety issues and incidents in line with the provision's child protection policy.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Reviewing filtering and monitoring alerts on a regular basis and ensuring that safeguarding concerns are acted upon promptly.
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the provisions Engagement for Learning Policy.
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/ or external services if necessary.
- Providing regular reports on online safety in provision to staff and wider stakeholders.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The Service Provider

The Service Provider working in collaboration with the Directors are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on provision devices and provision networks, which are reviewed and updated at least annually to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at provision, including terrorist and extremist material.
- Ensuring that the provision's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the provision's ICT systems on a fortnightly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the provision's Engagement for Learning Policy.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the provision's ICT systems and the internet (Appendix 2) and ensuring that learners follow the provision's terms on acceptable use (appendices 1 and 2).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by completing an electronic or paper copy of the safeguarding concern form.
- Following the correct procedures by liaising with the DSL and service provider if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the provisions Engagement for Learning Policy.
- Responding appropriately to all reports and concerns about sexual violence and/ or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- Exercising professional curiosity where online activity, communications, devices or behaviours indicate that a learner may be at risk of exploitation, grooming, criminal activity, radicalisation, self-harm, harmful sexual behaviour or mental health concerns.

This list is not intended to be exhaustive.

3.6 Parents/ Carers

Parents/ Carers are expected to:

- Notify a member of staff or the Directors of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the provision's ICT systems and internet (appendices 1 and 2).

Parents/ Carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and Members of the Community

Visitors and members of the community who use the provision's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating Learners About Online Safety

Learners will be taught about online safety as part of the curriculum:

All provisions have to teach:

- Relationships education and health education in primary provisions.
- Relationships and sex education and health education in secondary provisions.

Learners in **KS3** will be taught:

- To understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- To recognise inappropriate content, contact and conduct, and know how to report concerns.

Learners in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.
- Online safety education will also include emerging risks such as:
  - Sextortion
  - Deepfake images and videos
  - Online scams and financial exploitation
  - Misogynistic and extremist online content

- Risks associated with anonymous messaging platforms
- Online gambling and gaming-related risks
- Safe use of artificial intelligence tools

By the **end of secondary provision**, learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary at Leading Futures, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and learners with SEND.

Many learners attending Leading Futures may be particularly vulnerable to online harm because of SEND, communication difficulties, trauma, social isolation, emotional-based school non-attendance (EBSNA), autism, ADHD or other neurodiverse needs. Online safety education and intervention will therefore be personalised according to individual learner risk and need.

5. Educating Parents/ Carers About Online Safety

The provision will raise parents/ carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/ carers.

Online safety will also be covered during parent/ carer evenings.

The provision will let parents/ carers know:

- What systems the provision uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the provision (if anyone) their child will be interacting with online.

If parents/ carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Directors and/ or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Directors.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the provision behaviour policy)

6.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The provision will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their Tutor Groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education within our dedicated Learning for Life lessons, and other subjects where appropriate.

All staff, Directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The provision also sends information/ leaflets on cyber-bullying to parents/ carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the provision will follow the processes set out in the provisions Engagement for Learning Policy. Where illegal, inappropriate or harmful material has been spread among learners, the provision will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Confiscating and Examining Electronic Devices

The Directors, and any member of staff authorised to do so by the Directors, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners, and/ or
- Is identified in the provision rules as a banned item for which a search can be carried out, and/ or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other learners and staff. If the search is not urgent, they will seek advice from the Directors.
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the learner's co-operation.

The Directors may examine in the presence of parents/ carers, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/ or
- Undermine the safe environment of the provision or disrupt teaching, and/ or

- Commit an offence.

If inappropriate material is found on the device, it is up to Designated Safeguarding Lead and Directors to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, parents/ carers in the presence of the Directors may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/ or
- The learner refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of learners will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our Engagement for Learning Policy which includes guidance on searches and confiscation.

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the provision complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, learners and parents/ carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Leading Futures recognises that AI has many uses to help learners learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Leading Futures will treat any use of AI to bully learners very seriously, in line with our Anti-bullying and Engagement for Learning Policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the provision, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, learners and staff.

Staff must not enter personal, sensitive or confidential information relating to learners, families or colleagues into publicly available AI systems unless approved by the Directors and supported by appropriate data protection arrangements.

This includes, but is not limited to:

- EHCPs
- Safeguarding records
- Behaviour records
- Assessment data
- Medical information

- Personal identifying information

Any AI-generated content used within the provision must be reviewed by staff for accuracy, bias and suitability before use.

Learners may only use AI tools when directed or authorised by staff and must not use AI to misrepresent their own work.

Staff and learners should be aware of the risks associated with AI-generated deepfakes, manipulated images, voice cloning and misinformation.

7. Acceptable Use of the Internet in Provision

All learners, parents/ carers, staff, volunteers and Directors are expected to sign an agreement regarding the acceptable use of the provision's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the provision's terms on acceptable use if relevant.

Use of the provision's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners, staff, volunteers, Directors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

The provision reserves the right to monitor and review internet usage, search activity and safeguarding alerts generated through approved filtering and monitoring systems in accordance with safeguarding and data protection legislation.

8. Learners Using Mobile Devices in Provision

Learners may bring mobile devices into provision, but are not permitted to use them during:

- Lessons.
- Tutor group time.
- Clubs before or after provision, or any other activities organised by the provision.

Learners will be required to hand in their mobile devices each day on arrival to the provision. These will be returned at the end of the session.

Any use of mobile devices in provision by learners must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the provision Engagement for Learning Policy, which may result in the confiscation of their device.

9. Staff Using Work Devices Outside Provision

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the provision's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities. Staff must not use personal email accounts, cloud storage platforms or unapproved messaging applications for sharing learner information.

Only provision-approved systems and platforms should be used for communication with learners and families.

If staff have any concerns over the security of their device, they must seek advice from the Directors and Service Provider.

10. How the Provision Will Respond to Issues of Misuse

Where a learner misuses the provision's ICT systems or internet, we will follow the procedures set out in our policies on Engagement for Learning Policy and Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the provision's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct Policy, Staff Disciplinary and Grievance Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The provision will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, Directors and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/ hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure learners can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

All Directors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

11.2 Learners

All learners will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information.
- Password security.
- Social engineering.
- The risks of removable storage devices (e.g. USBs).
- Multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

Learners will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 4.

The DSL will maintain overview of:

- Emerging online risks
- Incidents and trends
- Filtering and monitoring concerns
- Vulnerable learner groups
- Actions taken to reduce identified risks

This register will be reviewed annually alongside the safeguarding risk assessment.

This policy will be reviewed every year by the Directors. At every review, the policy will be shared with all stakeholders. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks learners face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Engagement for Learning Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: KS3 and KS4 acceptable use agreement (learners and parents/ carers)

Acceptable Use Policy Learner Agreement Form

I have read and understood the Leading Futures Acceptable Use Policy.

I understand that the policy aims to:

- Set guidelines and rules on the use of the provision's ICT resources for staff, learners, Directors and, in part, parents/ carers
- Establish clear expectations for the way all members of the provision community engage with each other online
- Support the provision's policy on data protection, online safety and safeguarding
- Prevent disruption to the provision through the misuse, or attempted misuse, of ICT systems
- Support the provision in teaching learners about safe and effective internet and ICT use

As a learner, I will ensure:

- I will not use the provisions ICT devices in an unacceptable way (Section 6.3 of the policy), for example when using equipment to complete learning tasks or researching the internet
- I will keep my unique log-in and account information secure from my peers
- I will only access files that I am authorised to view or edit
- I will ensure my work email account(s) will only be used for work related business in my capacity as a learner. This may include contacting post-16 providers
- I will not use my personal mobile phones, cameras or ICT equipment in the provision
- I will seek permission from Directors to use personal devices within the provision
- I will not store personal music, videos and photos on devices that are the property of Leading Futures
- I will follow the guidance on social media, either for work or personal purposes, ensuring social media content is always appropriate
- I will not give the Wi-Fi password to anyone who is not authorised to have it
- I understand that my personal device will be confiscated, and police contacted, if staff suspect that there are images or data on the device that is banned under the Education Act 2011
- I understand that the provision can delete files and data found on searched devices if it is believed the data or file has been, or could be, used to disrupt teaching or break the provision's rules
- I will be vigilant when using the provisions ICT equipment remotely to uphold Data Protection Security, including the locking of devices and keeping devices secure
- I will hand any personal electronic devices to staff upon entry to the provision
- I understand that taking photographs or recordings within the provision are not permitted without specific permission

I am aware that monitoring and filtering systems are in place to ensure that Leading Futures staff and learners uphold the Acceptable Use Policy. This is maintained through:

- Data Protection Security
- Passwords
- Software Updates
- Firewalls
- Anti-Virus Software
- Restricted Access
- Encryption

As a learner I understand that unacceptable use of the provision's ICT facilities by any member of the provision community may result in disciplinary action in line with the Engagement for Learning Policy.

Learner signature: _____

Learner name printed: _____

Parent/ carer signature: _____

Parent/ carer name printed: _____ **Dat**

Acceptable Use Policy Parents/ Carers Agreement Form

I have read and understood the Leading Futures Acceptable Use Policy.

I understand that the policy aims to:

- Set guidelines and rules on the use of the provision's ICT resources for staff, learners, Directors and, in part, parents/ carers
- Establish clear expectations for the way all members of the provision community engage with each other online
- Support the provision's policy on data protection, online safety and safeguarding
- Prevent disruption to the provision through the misuse, or attempted misuse, of ICT systems
- Support the provision in teaching learners about safe and effective internet and ICT use

As a parent/ carer, I will ensure:

- I will not use the provisions ICT devices in an unacceptable way (Section 4 of the policy) if granted access to the provisions ICT facilities, for example for the purpose of a meeting or when visiting the provision
- I will keep unique log-in, and passwords issued to me by the provision secure
- I will not use my personal mobile phones, cameras or ICT equipment in the provision unless permission has been given by the Directors. For example, a learner performance
- I will not accept from staff or learners' personal emails or phone numbers
- I will not store personal music, videos and photos on devices that are the property of Leading Futures
- I will model for my son/ daughter how to communicate respectfully online with others, via the Leading Futures website and/ or social media channels
- I will follow the guidance on social media, either for work or personal purposes, ensuring social media content is always appropriate
- I will not use the provisions Wi-Fi unless specific authorisation is granted by the Directors. For example, working as a volunteer or to fulfil the purpose of the visit

I am aware that monitoring and filtering systems are in place to ensure that Leading Futures staff uphold the Acceptable Use Policy. This is maintained through:

- Data Protection Security
- Passwords
- Software Updates
- Firewalls
- Anti-Virus Software
- Restricted Access
- Encryption

As a parent/ carer I understand that unacceptable use of the provision's ICT facilities is vitally important. Any breach of this policy may result in Directors taking appropriate and proportional action.

Parent/ Carer member signature: _____

Parent/ Carer name printed: _____

Date: _____

Appendix 2: Acceptable Use Agreement (Staff, Directors, Volunteers and Visitors)

Acceptable Use Policy Staff Agreement Form

I have read and understood the Leading Futures Acceptable Use Policy.

I understand that the policy aims to:

- Set guidelines and rules on the use of the provision's ICT resources for staff, learners, Directors and, in part, parents/ carers
- Establish clear expectations for the way all members of the provision community engage with each other online
- Support the provision's policy on data protection, online safety and safeguarding
- Prevent disruption to the provision through the misuse, or attempted misuse, of ICT systems
- Support the provision in teaching learners about safe and effective internet and ICT use

As a staff member, I will ensure:

- I will not use the provisions ICT devices in an unacceptable way (Section 4 of the policy)
- I will keep my unique log-in and account information secure
- I will only access files that I am authorised to view or edit
- I will ensure my work email account(s) will only be used for work related business
- I will encrypt any sensitive information that needs to be sent to external individuals or organisations
- I will not use my personal mobile phones, cameras or ICT equipment in the provision
- I will not give personal emails or phone numbers to external stakeholders, learners, parents/ carers
- I will seek permission from Directors to use personal devices within the provision
- I will not use any device for personal use during contact time with learners
- I will not store personal music, videos and photos on devices that are the property of Leading Futures
- I will follow the guidance on social media, either for work or personal purposes, ensuring social media content is always appropriate
- I will not give the Wi-Fi password to anyone who is not authorised to have it
- I will be vigilant when using the provisions ICT equipment remotely to uphold Data Protection Security, including the locking of devices and keeping devices secure

I am aware that monitoring and filtering systems are in place to ensure that Leading Futures staff uphold the Acceptable Use Policy. This is maintained through:

- Data Protection Security
- Passwords
- Software Updates
- Firewalls
- Anti-Virus Software
- Restricted Access
- Encryption

As a staff member I understand that unacceptable use of the provision's ICT facilities by any member of the provision community may result in disciplinary action.

Staff member signature: _____

Staff member name printed: _____

Date: _____

Appendix 3: Online Safety Training Needs – Self-Audit For Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/ volunteer:	**Date**:
Question	**Yes/ No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in provision?	
Are you aware of the ways learners can abuse their peers online?	
Do you know what you must do if a learner approaches you with a concern or issue?	
Are you familiar with the provision's acceptable use agreement for staff, volunteers, Directors and visitors?	
Are you familiar with the provision's acceptable use agreement for learners and parents/ carers?	
Are you familiar with the filtering and monitoring systems on the provision's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the provision's ICT systems?	
Are you familiar with the provision's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/ further training?	
Do you understand the risks associated with artificial intelligence and deepfakes?	
Do you know how to report concerns arising from filtering and monitoring alerts?	
Are you aware of the signs of online grooming and sextortion?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Do you know the procedure for responding to a suspected nude or semi-nude image incident?	
Are you aware of current risks relating to online misogyny and extremist content?	
Are you confident adapting online safety education for learners with SEND?	

Appendix 4: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**