The right support, at the right time

Acceptable Use Policy

Author	**Mrs Emma Rennie-Gibbons**
Policy Adopted	**April 2025**
Policy Published	**April 2025**
Review Date	**July 2028**

This policy sets out the procedures and responsibilities for Acceptable Use of Devices at the Leading Futures Alternative Provision.

CONTENTS

1. Introduction and Aims

ICT and electronic devices are an integral part of the way our alternative provision works, and is a critical resource for learners, staff and Directors. ICT supports teaching and learning, pastoral and administrative functions of the provision. However, the ICT resources and facilities at our provision also pose risks to data protection, online safety and safeguarding.

This 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

This policy covers all users of our provision's ICT facilities, including Directors, staff and learners.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools

3. Definitions

ICT facilities	Includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
Users	Anyone authorised by the provision to use the ICT facilities, including Directors, staff and learners
Personal use	Any use or activity not directly related to the users' employment, study or purpose

Authorised personnel	Employees authorised by the provision to perform systems administration and/or monitoring of the ICT facilities
Materials	Files and data created using the ICT facilities including but not limited to documents,photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable Use

The following is considered unacceptable use of the provision's ICT facilities by any member of the provision community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the provision's ICT facilities includes:

- Using the provision's ICT facilities to breach intellectual property rights or copyright
- Using the provision's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the provision's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Sharing confidential information about the provision, its learners, or other members of the provision community
- Connecting any device to the provision's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the provision's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the provision's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the provision
- Using websites or mechanisms to bypass the provision's filtering mechanisms
- Participating in online gambling, using technology to facilitate betting, or accessing gambling websites. Such activities undermine the integrity of our systems and violate ethical standards

This is not an exhaustive list. The provision reserves the right to amend this list at any time.

The Directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the provision's ICT facilities.

4.1. Exceptions from Unacceptable Use
Where the use of provision ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Directors discretion, e.g. access to materials needed for teaching the lesson that would otherwise be blocked by the filtering system.

4.2. Sanctions
Learners and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the provision's policies on list policies.

Staff can find these policies at : Policies | Leading Futures

5. Staff (Including Directors)

5.1. Access to Provision ICT Facilities and Materials

The provision's Network Manager manages access to the provision's ICT facilities and materials for provision staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/ account information and passwords that they must use when accessing the provision's ICT facilities, with a forced update every 12 weeks.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Directors who will arrange for the Network Manager to provide access.

5.1.1. Use of Phones and Email

The provision provides each member of staff with a work email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the provision has provided.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of Contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the person responsible for Data Protection, Director of Service, immediately and follow our data breach procedure.

Staff must not share their personal email addresses with parents/ carers and learners, and must not send any work-related materials using their personal email account.

Staff must not give their personal phone numbers to parents/ carers or learners. Staff must use phones provided by the provision to conduct all work-related business.

The provision phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2. Personal Use

Staff are permitted to occasionally use provision ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused.

The Directors may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with learners
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no learners are present
- Does not interfere with their jobs, or prevent other staff or learners from using the facilities for work or educational purposes

Staff may not use the provision's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos). Staff should be aware that use of the provision's ICT facilities for personal use may put personal communications within the scope of the provision's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with this policy. Staff should be aware that personal use of ICT (even when not using provision ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where learners and parents/ carers could see them.

Staff should take care to follow the provision's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1. Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is
appropriate at all times. Accountant settings must have privacy controls in place at all times.

The provision has guidelines for staff, learners and parents/ carers on appropriate security settings for social media accounts (see appendix 1).

5.3. Remote Access

Staff can access the provision's ICT facilities and materials remotely. This is managed by the Network Manager and details on access are issued to staff on commencing employment at the provision. Access is made by an unpublished URL. Staff accessing the provision's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the provision's ICT facilities outside the provision and take such precautions as the Directors may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/ or subject to data protection legislation. Such information must be treated with extreme care and in accordance with GDPR guidelines outlined in our Data Protection Policy.

5.4. Social Media Accounts

The provision does have an official Facebook and LinkedIn page.
The provision does not have an official Instagram and/ or Twitter page.

5.5. Monitoring of Provision Network and Use of ICT Facilities

The provision reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/ access logs
- Any other electronic communications

Only authorised ICT staff with the permission of the Directors may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The provision monitors ICT use in order to:

- Obtain information related to provision business
- Investigate compliance with provision policies, procedures and standards
- Ensure effective provision and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Learners

6.1. Access to ICT Facilities

- Learners have access to computers and equipment in provision. These are available for use under the conditions in the Acceptable Use Policy.
- Learners are provided with an email address for the purpose of provision business.
- Learners are not permitted to use personal devices, including mobile phones and smart watches, to take photos or make recordings while on the premises. Learners are expected to hand such devices to staff upon entry into the provision, as outlined in the Engagement for Learning Policy.

6.2. Search and Deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, if the provision has suspicion that a learner(s) phones, computers or other devices hold pornographic images or any other data or items banned under provision rules or legislation, the phone will be confiscated and the police will be contacted. Staff will not search a learners phone as a safeguarding precaution for staff. The provision will advise parents/ carers of the incident.

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.

6.3. Unacceptable Use of ICT and the Internet Outside of Provision

The provision will sanction learners, in line with the Engagement For Learning Policy, if a learner engages in any of the following (even if they are not on provision premises):

- Using ICT or the internet to breach intellectual property rights or copyright Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the provision's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Sharing confidential information about the provision, other learners, or other members of the provision community
- Gaining or attempting to gain access to restricted areas of the provision network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the provision's ICT facilities
- Causing intentional damage to provision ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

This is not an exhaustive list. The provision reserves the right to amend this list at any time.

The Directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the provision's ICT facilities.

7. Parents/ Carers

7.1. Access to ICT Facilities and Materials

Parents/ carers do not have access to the provision's ICT facilities as a matter of course. However, parents/ carers working for, or with, the provision in an official capacity (eg, meeting or visitor) may be granted an appropriate level of access, or be permitted to use the provision's facilities at the Directors discretion.

Where parents/ carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2. Communicating With or About the Provision Online

We believe it is important to model for learners, and help them learn how to communicate respectfully with, and about, others online. Parents/ carers play a vital role in helping model this behaviour for their children, especially when communicating with the provision through our website and social media channels.

We ask parents/ carers to sign the agreement in appendix 2.

8. Data Security

The provision takes steps to protect the security of its computing resources, data and user accounts. However, the provision cannot guarantee security as situations can unfortunately arise. Staff, learners, parents/ carers and others who use the provision's ICT facilities should use safe computing practices at all times.

8.1. Passwords

All users of the provision's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Members of staff or learners who disclose account or password information may face disciplinary action. Parents/ carers who disclose account or password information may have their access rights revoked. Passwords are forced to revolve every 90 days.

8.2. Software Updates, Firewalls and Anti-Virus Software

All of the provision's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the provision's ICT facilities. Any personal devices using the provision's network must all be configured in this way.

8.3. Data Protection

All personal data must be processed and stored in line with data protection regulations and the provision's Data Protection Policy. The provision's GDPR guidelines outlined in our Data Protection Policy can be found on the provision's website at Policies | Leading Futures

8.4. Access to Facilities and Materials

All users of the provision's ICT facilities will have clearly defined access rights to provision systems, files and devices. These access rights are managed by the Network Manager and Directors.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Directors immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5. Encryption

The provision ensures that its devices and systems have an appropriate level of encryption. Provision staff may only use personal devices (including computers and USB drives) to access provision data, work remotely, or take personal data (such as pupil information) out of provision if they have been specifically authorised to do so by the Director using an encrypted USB or via remote access.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager and if they are presented to the Directors
.

9. Internet Access

The provision wireless internet connection is secured, filtered and monitored, with separate connections for staff, learners and visitors.

9.1. Parents/ Carers and Visitors

Parents/ carers and visitors to the provision will not be permitted to use the provision's wifii unless specific authorisation is granted by the Directors.

The Directors will only grant authorisation if:

- Parents/ carers are working with the provision in an official capacity (e.g. as a volunteer)
- Visitors need to access the provision's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result
in disciplinary action.

10. Monitoring and Review

The Directors and Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the provision.

This policy will be reviewed every 3 years.

The Directors are responsible for approving this policy.

11. Related Policies

This policy should be read alongside the provision's policies on:

- Child Protection and Safeguarding
- Engagement For learning
- Staff Code of Conduct, Discipline, and Grievance Policy
- Data Protection
- Working From Home

Appendix 1

Use of Social Media

Social media (e.g. Instagram, Twitter, LinkedIn etc.) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, and video sharing platforms such as YouTube, have social media elements to them also.

Leading Futures respects privacy and understands that staff, learners, and parents/ carers may use social media forums in their private lives. However, we believe that all should be mindful of personal communications that are likely to have a negative impact on professional standards and/ or the provision's reputation. We ask that all stakeholders follow the guidance below. Staff should pay particular attention to their personal use of social media.

Guidelines for managing your personal use of social media:

- Remember that nothing on social media is truly private.
- Social media can blur the lines between your professional and private life.
- It benefits everyone to act 'professionally' at all times - Keep content appropriate and consider your digital footprint and the impact it can have on your future.
- Keep your personal information private. Check your settings regularly and test your privacy settings.
- Regularly review your online friends/ connections – consider whether they are who they say they are and if you would trust them with details of your life.
- When posting online consider the scale, audience and permanency of what you post.
- Do not engage in conduct that would be viewed as unacceptable online. Obviously, do not use ethnic or religious slurs, insults or obscenities.
- Respect others' views and opinions. It is understandable that you may not always agree with opinions online, however, do not engage in a public disagreement. If you want to criticise, do it politely. Do not engage with trolls who aim to engage you in negative conversation.
- Be considerate of others' privacy and topics that could be considered personal, such as religion or politics.
- Do not share information about friends or colleagues without their prior consent.
- Do not discuss or disclose any information of a confidential nature on social media, especially information that pertains to Leading Futures' staff or learners.
- Do not attempt to discuss staff or learners in an 'anonymous' way.
- Be mindful of the material you consume and share, especially content that could potentially influence someone's perspective or harm others. This could include extremist or radicalised material.
- Be careful of fake news and sharing mis-information.
- Take control of your images – do you want to be tagged in an image? What would learners, staff, or parents/ carers say about you if they could see your images?
- If necessary, be quick to correct your own mistakes and admit when you are wrong.
- Know how to report a problem on the platforms you are using.

Appendix 2

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 appropriate at all times
- I will not give the wifi 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:

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 appropriate at all times
- I will not use the provisions wifi unless specific authorisation is granted by the Directors. For example, working as a volunteer or to fulfill 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:

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 wifi 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: **Date:**