lwetb
Bord Oideachais agus Oiliúna an Longfoirt agus na hIarmhí
Longford and Westmeath Education and Training Board

Title	**Third Party Access to LWETB ICT Systems and Resources**
Date	9th March, 2020
Approved by	LWETB Meeting 9th March, 2020
For Review By	LWETB Board

Third Party Access to LWETB ICT Systems and Resources

1. Purpose

The objective of this policy is to ensure that all third party organisations are made aware of their obligations as suppliers of services to LWETB. This document contains those parts of LWETB internal security policies that apply to third parties.

The purpose of this policy is to ensure that effective measures are in place to limit any exposure to LWETB.

2. Description

All third parties must comply with LWETB security requirements as set out in this document while using LWETB systems or data, and must implement security policies, standards & procedures to ensure that they fully comply with the requirements of this policy document, with current GDPR legislation, and with the related policies listed at the end of this document.

3. Definitions

“Third Party” is defined as any non-LWETB user or organisation accessing a service/platform provided by LWETB. This service may be on or off site.
“**Remote Access**” is defined as access to LWETB’s systems from any non-LWETB network or from the Internet whether on or off LWETB infrastructure.
“**Must**”, "**required**" or "**shall**", refer to an absolute requirement of the policy.
“**Must not**”, or "**shall not**", refer to statements which are an absolute prohibition of the policy.
“**Should**”, or "**recommended**" refer to a statement that should be applied. In certain circumstances, there may be a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.
“**Should not**”, or "**not recommended**" mean the specified behaviour should not be performed. There may be valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour so described.

4. Requirements

The following security controls apply:

1. Third parties must sign an agreement, either as an addendum to any existing Service Level Agreement, or as a stand-alone document, in which LWETB’s standards for ICT security and Data Protection are detailed, and to which this policy is added as an appendix.

The following criteria must be included in all agreements:

- A statement of compliance with LWETB security policies.
- A suitable Non-Disclosure Agreement (NDA), if applicable e.g. personal information is exchanged or LWETB intellectual property is divulged.
- Security responsibilities must be clearly defined including the security controls applied to LWETB data. **This is also a legal requirement where personal data may be processed**.
- A notification procedure and security incident management.
- Right to audit and monitor compliance with the security requirements and controls of the agreement.
- Arrangements for the return or destruction of the information on completion of the agreement.
- Change management procedure.
- Service level and acceptable parameter indicators.
- Data Protection elements:
    - Specifying the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller
    - the third party guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and to ensure the protection of the rights of the data subject;
    - the third party ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
    - the processor agrees to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

2. The third party must communicate a “General User Security Policy” to its staff at least annually. In addition, the following summary information should be communicated regularly:

- All LWETB information must be treated as confidential – sensitive data (e.g. client or PPS No.) must never be copied onto a non-LWETB system unless as part of an approved business process. All systems or devices containing LWETB data must be housed securely, and must not be brought outside approved working areas.
- All LWETB computers & media must be disposed of securely – LWETB data must be securely wiped prior to equipment disposal.
- Third parties may only use login accounts that have been issued explicitly for their use.
- Systems development activities must comply with guidelines and standards issued by LWETB
- All proposed ICT work must be agreed with LWETB before commencement

4.1 User Virus Protection

Antivirus software must be installed on all computers that connect to LWETB systems or host LWETB data and must be automatically updated to ensure LWETB is protected from the latest security threats. Exceptions may be made for operating systems that are considered at low risk from malware.

4.2 Internet Usage

- Third parties accessing the internet via LWETB systems or using LWETB equipment are expected to be responsible and to avoid actions that cause interference or disruption to others.
- All internet users must be subject to monitoring & content filtering. LWETB reserves the right to review internet browsing via LWETB systems to ensure compliance with policy, regulatory & legal requirements.
- Content filtering must be configured to block web sites containing illegal or inappropriate content – including potentially illegal, defamatory, abusive, obscene, profane, racist, sectarian or pornographic words, pictures, or any materials which may cause offence or annoyance to any reasonable person.
- Third parties may not access copyrighted information in a way that violates the copyright – third parties should ensure that they read & comply with any copyright notices on any materials they are accessing, copying or printing.
- Third parties may not post information to social media sites, external bulletin boards, websites, blogs or discussion forums in the name of LWETB or purporting to represent the views of LWETB. They may not post information to websites or discussion forums that discuss or disparage LWETB policies, products or personnel.
- Third parties may not change the settings of LWETB systems or use LWETB equipment in an attempt to bypass the monitoring & filtering implemented by LWETB.
- LWETB reserves the right to refer any serious breach of acceptable internet use to An Garda Síochána.

4.3 User Portable Device Security

LWETB contractors & third parties using laptops, smart-phones, tablets, USB memory sticks, CDs or other portable devices containing LWETB data must take appropriate steps to ensure the security of that data.

Sensitive data (e.g. customer data) must never be stored on a laptop or portable disk unless it is encrypted using LWETB approved encryption software.

Laptops or portable devices and storage media or related printed material must never be left unattended and must be locked away when not in use. They must not be brought outside LWETB-approved working areas unless for authorised business purposes.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisational Support & Development	Revisions and updates to the policy
LWETB Management Team	Approval of the Policy
Data Owners	Ensuring implementation of policy.
Internal and external audit	Monitoring and reporting compliance with the policy

6. Related Documents

- Data Protection Policy
- Password Acceptable Usage Policy
- Remote Access Policy
- Asset Protection Policy
- Logical Access Policy
- Encryption Policy
- Anti-Virus and Malware Protection Policy
- ICT Acceptable Usage Policy