



Online Safety Policy

Author/Owner	Gemma Kennedy
Consulted with	WEC Group HR Department
Consultation date	26/11/2025
Date of approval	26/11/2025
Approved by	Group Managing Director
Next review	25/11/2026

Table of Contents

Policy Purpose	3
Policy Scope	3
Our Values	3
Key Objectives	3
Roles and Responsibilities	4
The WEC Engineering Academy Online Safety Coordinator	4
The Managing Director	4
ICT Support staff	5
Engineering Academy Management Team	5
Managing Information Systems	5
Securely Maintaining information	5
Filter Management	6
Employees use of personal devices	6
Designated Safeguarding Officer	7
Employees including Apprentices	7
ICT support staff	7
Use of facilities for curriculum teaching and learning	7
General Data Protection and Online Safety	8
Review and Evaluation	8
Useful Contacts	9

Policy Purpose

The WEC Group online safety policy aims to create an environment where all our employees including our apprentices, work together to inform each other of ways to use the internet responsibly, safely and positively.

Through using ICT, we equip our employees including our apprentices to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable our employees to find, explore, analyse, exchange and present information in varied and stimulating ways.

Internet technology helps our apprentices to learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all WEC Group employees including apprentices. The online safety policy encourages appropriate and safe conduct and behaviour when achieving this.

Policy Scope

The Apprentice Engineering Academy online safety policy applies to all employees and apprentices of the wider WEC Group business who have access to or maintain WEC Group related Internet, computer systems and mobile technologies internally and externally.

The WEC Group will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage within the WEC Group.

Our Values

The WEC Group values are:

- 1) **INTEGRITY**- We will operate ethically, reliably and honestly.
- 2) **EXCELLENCE**- We will exceed expectations and strive to be the best we can.
- 3) **POSITIVITY**- We will bring energy and enthusiasm to both our work and learning whilst being supportive of others, our processes, our customers and the Company.
- 4) **TEAMWORK**- We will work together to be more efficient and productive, resulting in increased innovation, higher morale and improved retention.
- 5) **SAFETY**- We will promote a safety culture within the workplace which is fundamental to our operational excellence.

We align our values to the British Values, which are:

- 1) **Democracy**- giving everyone a voice of opinion
- 2) **Individual liberty**- Freedom of speech
- 3) **The Rule of Law**- No one is above the law, innocent until proven guilty
- 4) **Respect and Tolerance**- respect for people of all backgrounds, cultures, ages, genders, faiths, sexualities and beliefs

Key Objectives

The key objectives of this Policy are to cover:

- WEC Group based ICT systems (including the Learner Management System, Aptem) and equipment
- WEC Group based intranet and networking

- WEC Group related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal WEC Group networking, such as webmail, network access, file-serving document folders and printing.
- WEC Group ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Apprentice's and employee's personal ICT equipment when used on WEC Group premises and which makes use of networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the WEC Group site.

Roles and Responsibilities

Monitoring the online safety Policy

In the event of an online safety incident at the Engineering Academy, the following people will be informed:

- Online safety Coordinator/Officer (Ian Bray)
- Academy Training Manager (Kris Mercer)
- Designated Safeguarding Lead (Edd Belshaw)
- HR Manager (Gemma Kennedy)

The WEC Engineering Academy Online Safety Coordinator

The WEC Engineering Academy has a designated Online Safety Coordinator, Ian Bray who reports to the Service Centre Manager's and Governors and coordinates online safety provision across the WEC Group. The coordinator liaises with Service Centre Managers, the Engineering Academy Training Manager, the Designated safeguarding lead and other senior managers as required.

- The Engineering Academy online safety coordinator is responsible for online safety issues on a day-to-day basis.
- The Engineering Academy online safety coordinator maintains a log of submitted online safety reports and incidents (these will be logged on the safeguarding, prevent and online safety database).
- The Engineering Academy online safety coordinator audits and assesses employee's online safety training, and ensures that all staff are aware of their responsibilities and the Engineering Academy online safety procedures.
- The coordinator is also the first port of call for staff requiring advice on online safety matters.
- Although all employees are responsible for upholding the WEC Group online safety policy and safer internet practice, the online safety coordinator and ICT support are responsible for monitoring internet usage by employees including apprentices on Company property, such as laptops, even those used off-site.
- The online safety coordinator is responsible for promoting best practice in online safety within the wider WEC Group

The Managing Director, Steve Hartley

The WEC Group Managing Director is responsible for online safety. The online safety coordinator will liaise directly with the Managing Director with regard to reports on online safety effectiveness, incidents,

monitoring, evaluation and developing and maintaining links with local stakeholders and the wider community.

ICT support staff

Internal ICT support employees are responsible for maintaining the Engineering Academy networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the WEC Group system, particularly file-sharing and access to the Internet is secure. They further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.

Engineering Academy Management Team

The Engineering Academy management team need to ensure that they are aware of the current WEC Group's online safety policy, practices and associated procedures for reporting online safety incidents.

- All staff need to follow the WEC Group social media policy, in regard to external off-site use, personal use (mindful of not bringing the WEC Group into disrepute), possible contractual obligations, and conduct on Internet company messaging or communication platforms, for example email and the WEC Group website.
- All Management staff need to rigorously monitor apprentice Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the Engineering Academy site.
- The Engineering Academy Management team should be aware of online propaganda and help apprentices with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted.

Managing information systems

Securely maintaining information

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of all WEC Group employees including apprentices.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions. Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date; through regular monthly patching
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured- the IT department are responsible for this.

Wide Area Network (WAN) security issues include:

- The Engineering Academy broadband firewalls are configured to prevent unauthorised access.
- Decisions on WAN security are made with the IT department.

The Engineering Academy broadband network is protected by a suitable high-performance active firewall at the Internet connecting nodes.

- The security of the Engineering Academy information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used unless it has been encrypted and virus checked
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the network will be regularly checked.
- System capacity in relation to storage will be checked regularly.
- The use of user logins and passwords to access the network will be enforced.

Filter management

- The Engineering Academy's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.
- Any breaches in filtering should be reported to the ICT Support and/or emailed to the IT Manager: ian.bray@wecl.co.uk
- If employees including apprentices discover unsuitable sites, the URL will be reported to the IT Manager who will then record the incident and escalate the concern as appropriate.
- The WEC Academy's filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the Engineering Academy's filtering policy will be risk assessed by staff with technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The WEC Group Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the WEC Group believes is illegal will be reported to appropriate agencies.

Employees use of Personal Devices

All WEC Group employees including apprentices are not permitted to use their own personal phones or devices for contacting apprentices, young people and their families within or outside of the setting in a professional capacity.

Employees including apprentices will be issued with a WEC Group chrome book. Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices (other than the chrome books) will not be used during teaching periods unless permission has been given by a member of the Engineering Academy Leadership Team in emergency circumstances.

If members of the management team have an educational reason to allow apprentices to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Training Academy Manager.

WEC Group employees should not use personal devices such as mobile phones or cameras to take photos or videos of learners and will only use work-provided equipment for this purpose.

If a member of staff breaches this clause, then disciplinary action may be taken.

Designated Safeguarding Officer:

The Designated Safeguarding Officer is trained in specific online safety issues.

The Designated Safeguarding Officer can differentiate which online safety incidents are required to be reported to, local Police, Local Safeguarding team, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

Possible scenarios might include:

- Allegations against members of staff.
- Computer crime – for example hacking of WEC Group systems.
- Allegations or evidence of 'grooming'.
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Producing and sharing of Youth Produced Sexual Imagery (YPSI)

Employees including Apprentices:

- Employees including Apprentices need to be aware of how to report online safety incidents at the WEC Group, and how to use external reporting facilities.
- Employees including Apprentices need to make themselves aware of the online safety posters which are situated in the Academy Classrooms.

ICT support staff:

- IT support staff will ensure that bought in hardware and software solutions feature built in training provision.
- IT technical support staff and network managers have relevant industry experience.

Policy guidance for handling personal data, dealing with freedom of information requests, and complying with privacy regulations pertaining to website data:

- All of these areas are regulated by the Information Commissioner (ICO), and every UK organisation has to comply with the responsibilities and obligations as defined by the ICO. The WEC Group are no different to any other organisation in this regard. The ICO guidance on how to comply with these obligations is updated regularly. The WEC Group refer directly to this guidance in these areas.

When disposing of computer equipment, The WEC Group needs to ensure all data, including personal data is wiped.

Use of IT facilities for curriculum teaching and learning:

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, Learners should be trusted to be responsible when researching the Internet, and delivery staff will consider the age and maturity of the learners.

General Data Protection and online safety:

The GDPR sets out the **key principles** that all personal data must be processed in line with.

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected
- There are also **stronger rights for individuals** regarding their own data.
- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.
- The General Data Protection Act is relevant to online safety since it impacts on the way in which personal information should be secured on the WEC Group computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
- Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the WEC Group and external stakeholders, particularly, but not exclusively: learners, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network.
- Personal data should only be stored on secure devices. In other words, only computers, servers, file-servers, cloud space, or devices which require a user name and password to access the information. Secure accounts need to be logged off after use to prevent unauthorised access.
- Personal e mails must not be used for WEC Group business.

Online safety policy review and evaluation schedule:

The WEC Group senior leadership team is responsible for determining, evaluating and reviewing the online safety policy to encompass teaching and learning, use of WEC Group IT equipment and facilities by apprentices, employees and visitors, and the agreed criteria for acceptable use by apprentices, WEC Group staff and governors of Internet capable equipment for WEC Group related purposes or in situations which will impact on the reputation of the WEC Group, and/or on WEC Group premises.

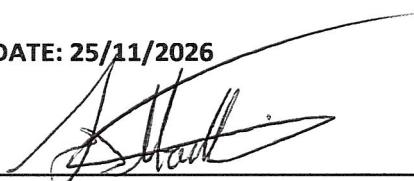
The online safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, technological and Internet developments, current government guidance and WEC Academy related online safety incidents.

Online safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the Engineering Academy. The leadership team is encouraged to be aspirational and innovative in developing strategies for online safety provision.

This online safety policy will be reviewed annually- additional reviews may be needed during the year in the event of any online safety incidents.

NEXT REVIEW DATE: 25/11/2026

SIGNED: _____



DATE: _____

26/11/25.

Steve Hartley, Managing Director

Useful Contacts

IT Department: The WEC Engineering Academy Online Safety Coordinator Ian Bray, Group IT Manager	07525 668082	ian.bray@wecl.co.uk
WEC Group Engineering Academy Governing Team: Steve Hartley- Chair of Governors Gemma Kennedy- Governor Jamie Sharp- Governor Neil Burrows Chris Dickinson Derrick Connelly	07774 768342 07384 460546 07464 547412 Contact via Gemma Kennedy	steve@wecl.co.uk gemma.kennedy@wecl.co.uk jamies@mtladv.com
WEC Group Safeguarding officers/ Prevent: Edd Belshaw, Prevent Lead Gemma Kennedy Kris Mercer Naomi Coates Phil Hosey Jason Bradder	07803 591837 07384 460546 07493 969929 07384469942 01254 773718 01254 773718	Edd.Belshaw@wecl.co.uk Gemma.kennedy@wecl.co.uk Kris.mercer@wecl.co.uk NaomiC@mtladv.com phil.hosey@wecl.co.uk jasonb@mtladv.oc.uk
Human Resources: Gemma Kennedy, Group HR Manager Naomi Coates, MTL HR Manager	07384 460546 07384 469942	Gemma.kennedy@wecl.co.uk Naomic@mtladv.com