Online Safety Policy

This policy is effective in Lancaster Academy , part of the Learning without Limits Academy Trust

Associated Policies:	
Lancaster Academy Behaviour Policy	Social Media Policy
Child Protection and Safeguarding Policy	Staff Behaviour (Code of Conduct) Policy
Data Protection Policy	Staff Expectations Policy
Equality, Diversity and Inclusion Policy	Whistleblowing Policy
Recruitment Policy	

Version: 2.2	**Status: LIVE**
Date: January 2024	**Next Review: January 2025**

Version	**Date**	**Author**	**Changes**
V1.0	November 2021	KK/DG	New Trust wide policy created, based on the latest LCC policy (Aug 2017).
V1.1	December 2021	AE/DG	Addition of Acceptable Use Arrangements for Learners and Loan Agreement Terms for LwLAT devices in appendices.
V2.1	November 2022	AE	New format of front sheet. Section 11 Remote Learning updated to refer more generally to a pandemic, such as Covid-19. Addition of Section 13 Radicalisation.
V2.2	January 2024	AE	Trust template policy for local adaptation. List of Associated Policies updated. Reference to 'Director IT and Estates' updated to Chief Operating Officer. Reference to KCSiE updated to 2023. All references to pupil, student, children or young person updated to learner. Section 13 – Artificial Intelligence added. Additional wording related to filtering added to 21.1, Section 21 Monitoring Arrangements. All Acceptable Use Agreement Appendices removed from policy.
V2.2a	January 2024	SA	Localised version for use at Lancaster Academy. Agreed by Hilary Slocombe, Chair of Governors

This document is a Trust wide policy which is approved by Trustees for use in all Trust premises. It is the responsibility of individual Academies to insert information in to the document where indicated so that it is relevant to local circumstances and practice, whilst not removing any content contained within it, prior to the policy being noted by Local Governing Bodies.

Contents

1. Aims ... 3
2. Objectives ... 3
3. The 4 Key Categories of Risk ... 3
4. Scope of this policy ... 3
5. Who is responsible for carrying out this policy ... 4
6. Legislation and guidance ... 4
7. Equality statement ... 4
8. Roles and responsibilities ... 5
8.1. The Principal ... 5
8.2. The Designated Safeguarding Lead (DSL) ... 5
8.3. Senior IT Technician ... 6
8.4. All staff and volunteers ... 6
8.5. Parents and Carers ... 6
8.6. Visitors and members of the community ... 7
9. Educating learners about online safety ... 7
10. Educating parents and carers about online safety ... 8
11. Remote learning ... 8
12. Cyber-bullying ... 8
12.1. Definition ... 9
12.2. Preventing and addressing cyber-bullying ... 9
13. Artificial Intelligence (AI) ... 9
14. Radicalisation ... 10
14.1. Definition ... 10
14.2. Preventing and addressing radicalisation ... 10
15. Examining electronic devices ... 10
16. Acceptable use of the internet in the Academy ... 11
17. Learners using mobile devices in the Academy ... 11
18. Staff using work devices outside the Academy ... 11
19. How Academies will respond to issues of misuse ... 12
20. Training ... 12
21. Monitoring arrangements ... 13
22. LwLAT Wellbeing Statement ... 13
23. Review of this Policy ... 13

1. Aims

1.1. All Academies within the Learning without Limits Academy Trust (LwLAT) are committed to online safety. Whilst we acknowledge the range of exciting opportunities available online we recognise that there are new and changing threats to learners and their safety whilst online. The aim of this policy is to facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare learners and learner for the risks and opportunities of today's and tomorrow's digital world.

2. Objectives

2.1. All Academies within the LwLAT will:

- Have robust processes in place, including filtering and monitoring systems, to ensure the online safety of learners, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy 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

3. The 4 Key Categories of Risk

3.1. Our approach to online safety is based on addressing the following categories of risk (KCSIE 2023):

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

4. Scope of this policy

4.1. This policy applies to trustees and governors, all teaching, non-teaching, support staff, supply staff, peripatetic and contract staff, volunteers, contractors and external service or activity providers working in or on behalf of the Academy including, extended Academy and off-site activities.

5. Who is responsible for carrying out this policy

5.1. The implementation of this policy will be monitored by the Principal of each Academy.

5.2. Line Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

5.3. All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it.

6. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

6.2. It also refers to the DfE's guidance on protecting children from radicalisation: The Prevent Duty.

6.3. 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.

6.4. The policy also takes into account the National Curriculum computing programmes of study and:

- Teaching Online Safety in Schools
- Education for a Connected World - A Framework to Equip Children and Young People for Digital Life

6.5. This policy complies with our funding agreement and articles of association.

7. Equality statement

7.1. Some learners have an increased risk of abuse, and additional barriers can exist for some learners with respect to recognising or disclosing it. We are committed to anti-discriminatory practice and recognise learners' diverse circumstances. We ensure that all learners have the same protection, regardless of any barriers they may face. (LwLAT Child Protection and Safeguarding Policy September 2021).

8. Roles and responsibilities

8.1. The Principal

8.1.1. The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy including:

- Fostering a culture of safeguarding where online safety is fully integrated into whole Academy safeguarding
- Overseeing and working with the Designated Safeguarding Lead (DSL)
- Ensuring that policies are followed by all staff
- Take overall responsibility for data management and information security
- Ensuring the Academy works with the LwLAT Chief Operating Officer and implements and makes effective use of appropriate IT systems and services including filtering and monitoring, protected email systems and that all technology including cloud based systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of learners, including risk of learners being radicalised
- Ensure that there is a system in place to monitor and support staff who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the Academy's arrangements for online safety
- Ensure the Academy website meets statutory requirements

8.2. The Designated Safeguarding Lead (DSL)

8.2.1. Details of the Academy's DSL and deputy DSLs (DDSLs) are set out in the Academy's Child Protection and Safeguarding Policy as well as relevant job descriptions.

8.2.2. The DSL takes lead responsibility for online safety in Academy, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the Principal, LwLAT IT Support and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Academy's Child Protection Policy
- Ensuring that any online safety incidents are logged (see Appendix 5) 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 Academy behaviour policy
- Updating and delivering staff training on online safety (Appendix 4 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 Academy to the Principal and/or governing body

8.2.3. This list is not intended to be exhaustive.

8.3. Senior IT Technician

8.3.1. Overall responsibility for IT across the LwLAT lies with the Chief Operating Officer.

8.3.2. The IT manager at each Academy will work closely with the Chief Operating Officer and the Trust Technical Systems Manager to ensure the Academy:

- Has an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Has IT systems which are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducts a full security check and monitoring the Academy's IT systems on a regular basis
- Blocks access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Logs any online safety incidents (see Appendix 5) and dealt with appropriately in line with this policy
- Deals with any incidents of cyber-bullying appropriately in line with the Academy Behaviour Policy

8.3.3. This list is not intended to be exhaustive.

8.4. All staff and volunteers

8.4.1. 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 Academy's IT systems and the internet, and ensuring that learners follow the Academy's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Being aware of the Academy's Behaviour 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'

8.4.2. This list is not intended to be exhaustive.

8.5. Parents and Carers

8.5.1. Parents and carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's IT systems and internet

8.5.2. Parents and carers can seek further guidance on keeping learners safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre
- Hot topics Childnet International
- Parent resource sheet Childnet International
- Healthy relationships Disrespect Nobody

8.6. Visitors and members of the community

8.6.1. Visitors and members of the community who use the Academy's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

9. Educating learners about online safety

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

- National Curriculum computing programmes of study.
- Guidance on relationships education, relationships and sex education (RSE) and health education.

9.2. **All** LwLAT Academies will teach:

- Relationships education and health education in primary academies
- Relationships and sex education and health education in secondary academies

9.3. In **Key Stage 3**, learners will be taught to:

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

9.4. Learners in **Key Stage 4** will be taught to:

- 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

9.5. By the **end of secondary education**, 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 which 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 which 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)

9.6. The safe use of social media and the internet will also be covered in other subjects where relevant. It will also be covered in assemblies, "Stop The Clock" lessons and as part of the PSHE programme.

9.7. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable learners, victims of abuse and some learners with SEND.

10. Educating parents and carers about online safety

10.1. The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. Parents and carers can also access training and advice from National Online Safety and through the Academy 'Wakeup Wednesday' advice available weekly.

10.2. This policy will also be shared with parents.

10.3. Online safety will also be covered during parents' evenings.

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

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

11. Remote learning

11.1. All LwLAT academies recognise that during a national pandemic, such as COVID-19, they may have to deliver lessons remotely. In this instance all Academies will follow the LwLAT Blended and Remote Learning Education Policy.

12. Cyber-bullying

12.1. Definition

12.1.1. 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also each Academy's behaviour policy.)

12.2. Preventing and addressing cyber-bullying

12.2.1. 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. This will be reinforced in assemblies and form time as well as PSHE.

12.2.2. The Academy 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, and other subjects where appropriate, particularly ICT lessons.

12.2.3. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training.

12.2.4. The Academy also displays information/leaflets in reception on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support learners who may be affected.

12.2.5. In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, the Academy will use all reasonable endeavours to ensure the incident is contained.

12.2.6. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

13. Artificial Intelligence (AI)

13.1. Lancaster Academy recognises that AI has many uses to help children 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.

13.2. Lancaster Academy will treat any use of AI to bully pupils in line with both our anti-bullying and behaviour policy.

13.3. We will update this policy in line with the Online Safety Act 2023 as and when relevant guidance is issued by the DfE.

14. Radicalisation

14.1. Definition

14.1.1. Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

14.2. Preventing and addressing radicalisation

14.2.1. Lancaster Academy recognises that learners can be vulnerable to radicalisation online. We understand that protecting learners from the risk of radicalisation should be seen as part of our wider safeguarding duties and is similar in nature to protecting them from other harms.

14.2.2. All staff and governors will be made aware of the risks posed by the online activity of extremist and terrorist groups.

14.2.3. Staff will receive training on identifying learners who may be vulnerable to radicalisation and know what to do when they are identified.

14.2.4. Learners will have access to teaching and support and advice on how to keep themselves safe online, including signposting to support.

14.2.5. The DSL will contact the Prevent team for advice and support where there are concerns that a learner may be being radicalised. In an emergency the police will be contacted.

15. Examining electronic devices

15.1. Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on learners' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

15.2. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the Academy rules

15.3. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
- Report it to the police*

15.4. ** Staff may also confiscate devices for evidence to hand to the police, if a learner discloses that they are being abused and that this abuse includes an online element.*

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nude and semi-nudes: advice for education settings working with learners and learner
- The Academy's COVID-19 risk assessment

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

16. Acceptable use of the internet in the Academy

16.1. All learners, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's IT systems and the internet. Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

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

16.3. We will monitor the websites visited by learners, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

16.4. More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

17. Learners using mobile devices in the Academy

17.1. Learners may bring mobile devices into Academy and use them at lunch and break but are not permitted to use them during:

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

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

17.3. Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the Academy behaviour policy, which may result in the confiscation of their device.

18. Staff using work devices outside the Academy

18.1. 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- 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

18.2. Staff members must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in Appendix 3.

18.3. Work devices must be used solely for work activities.

18.4. If staff have any concerns over the security of their device, they must seek advice from The IT Technician team, or from the Trust's team.

19. How Academies will respond to issues of misuse

19.1. Where a learner misuses the Academy's IT systems or internet, we will follow the procedures set out in our Behaviour Policy and Acceptable Use Agreements. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

19.2. Where a staff member misuses the Academy's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Trust's Disciplinary Procedures with reference to the Acceptable Use Agreement, the Trust's Staff Behaviour (Code of Conduct) Policy, Staff Expectations Policy and Social Media Policy found on the Trust website. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

20. Training

20.1. 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.

20.2. 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).

20.3. 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 learners are at risk of online abuse
- Learners can abuse their peers online through:
  - Abusive, 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

20.4. Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

20.5. 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 the risks up
- develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term

20.6. The DSL team 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 on the subject of online safety at regular intervals, and at least annually.

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

20.8. Volunteers will receive appropriate training and updates, if applicable.

20.9. More information about safeguarding training is set out in our child protection and safeguarding policy.

21. Monitoring arrangements

21.1. The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5. Issues involving learners will be logged on CPOMS. Issues regarding members of staff may initially logged as a low level concern or as be managed as part of the allegations process.

21.2. This policy will be reviewed yearly by the LwLAT DSL and academies, alongside the Trust's Chief Operating Officer. After every review the policy will be shared with the local governing body. The review will be supported by an annual risk assessment that considers and reflects the risks learners face online.

21.3. All academies within the LwLAT will also review their online safety policy and practice using 360 Degree Safe 360DegreeSafeAudit

22. LwLAT Wellbeing Statement

22.1. The Trust will always put the effective education of our learners at the heart of any decision that we make. In doing so, we recognise that the requirement to adhere to policies and procedures may be time consuming and can impact on workload. For this reason the Trust and its Academies will always endeavour to support staff when policies and procedures are being actioned.

23. Review of this Policy

23.1. The LwLAT Trust Board has overall responsibility for the adoption, review and amendments of this policy. The Trust Board will review the policy annually, or earlier if required by legislature changes.