[illegible]	[illegible]

Version: 1.2	**Status: LIVE**
Date: November 2022	**Next Review: November 2023**

Contents

2. O

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

Pg(e)-3 (us)-4 3 (h)-(
11.04 0 0 11.04 114.6 624.12 Tm<0078>Tj(v)_0 1 Tf 1935 0 Td( )Tj0.

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 pupils, including risk of children 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 Director of IT & Estates.

8.3.2. The IT manager at each Academy will work closely with the Director of IT & Estates and the 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

can also access training and advice from National Online Safety and through the Academy 'Wakeup Wednesday' advice available weekly.

10.1.2. This policy will also be shared with parents.

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

10.1.4. 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.

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

11. Remote learning

11.1.1. 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

[Adapt this sub-section to reflect your Academy's approach.]

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

12.3.2. The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups.

12.3.3. 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. [Add your Academy's approach.]

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

12.3.5. The Academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. [Add/amend/delete]

14.3. 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*

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

14.4. Any searching of pupils 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 children and young people
- The Academy's COVID-19 risk assessment

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

15. Acceptable use of the internet in Academy

15.1. All pupils, 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.

15.2. 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.

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

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

16. Pupils using mobile devices in the Academy

[Adapt this section to reflect your Academy's approach. Include any changes to your rules to allow pupils to use the NHS COVID-19 app.]

16.1. Pupils may bring mobile devices into Academy, 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

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

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

Acceptable use of the Academy's IT systems and internet: Agreement for pupils and parents/carers

Parent/carer's agreement: I agree that my child can use the Academy's IT systems and

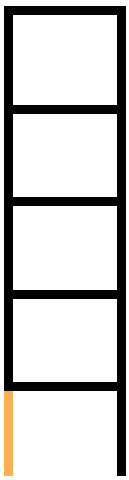
Appendix 4: Online Safety Training needs – Self Audit for Staff

[To be adapted]

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 the Academy?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the Academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the Academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the Academy's IT systems?	
Are you familiar with the Academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help



I know people online sometimes tell lies.

They might lie about who they are or where they live.

My trusted adults are _____  at school

My trusted adults are _____  at home

My name is _____

LwLAT Acceptable Use Arrangements for Students

This document states the rules all student users of:

- Academy or Trust ICT (information and communications technologies) resources must abide by
- Academy computer and internet accounts must abide by and the consequences for breaking them

These arrangements aim to:

- Define and identify unacceptable use of the Academy ICT systems and external systems
- Educate users about their data security responsibilities
- Describe why monitoring of the ICT systems may take place
- Define and identify unacceptable use of social networking sites and Academy or Trust devices
- Specify the consequences of non-compliance

These arrangements apply to all students and all users of the Learning without Limits Academy Trust ICT systems who are expected to read and understand these arrangements. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which a

Network access and security

All user account details are for the exclusive use of the individual to whom they are allocated. All students are responsible for ensuring their password remains confidential and their account is secure. Students must not ask for another student's password. Students are encouraged to change their password regularly (every 90 days).

Users should only access areas of the Academy's computer systems to which they have authorised access.

Under no circumstances should anyone else be allowed to use an electronic device or computer account provided by the Academy, unless being directly supervised by a parent or a member of staff.

Laptops and other devices must never be left unattended on the Academy premises or in a public place. A stolen device must be reported to the police and a crime reference number obtained. Lost or stolen devices must be reported to the Academy immediately.

Academy email

Where email is provided, it is for academic use only.

The Academy's email system can be accessed from both the onsite computers, and via the internet from any computer. Wherever possible, all Academy related communication must be via the user's Academy email address.

The sending of emails is subject to the following rules:

- Language must not in13.6 (m)ye1 (d)-03 (c)-esmg-4.9 (a)rem10.6 (o)-9.6 (r)-3.2 (d)-4.3 (s)e otde 10.6 (o)f0.7 (a)f3.

Internet Access

Internet access is provided for academic use only.

All Academies' internet connections are filtered, meaning that a large amount of inappropriate material is n

Appendix 8

Agreement Terms for any device loaned by LwLAT: Agreement for pupils and parents/carers

- Should you move address from the location you have given us, it is essential that you inform your Academy at the earliest opportunity.
- You will be issued with a laptop, power supply and protective case. These remain the property of the Learning without Limits Academy Trust.
- You will be able to install approved equipment such as printers and scanners on your computer. At no point must you open the computer and make changes to the inner hardware.
- The computer and any connectivity equipment must be used in accordance with the Acceptable Use Policy. Equipment must not be used for any illegal and/or antisocial purpose.
- There may be occasions when we need you to return the computer to an Academy for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the computer. The Learning without Limits Academy Trust cannot be held responsible for the loss or damage of any data on the computer during this process. It is your responsibility to return the computer to the Academy.

During this process, technical members of staff may view data or programmes on the computer. You will be held responsible to the acceptable use policy at this point. You may want to remove personal data from the computer before its return.

- All technical support and maintenance must go through the Academy your child attends.
- If your computer is stolen you must immediately report it to the police and get a crime reference number. Immediately report this to us; we will make every effort to replace the computer if we are able.

If your computer is accidentally damaged, immediately contact us. We will do our best to repair the damage, if this is not possible, replacement will be on a case by case basis.

Responsibilities you have to care for your computer

- You have a responsibility to take reasonable care to ensure the security of the computer and connectivity equipment.
- You must not decorate or change the external face of the equipment provided in any way, including affixing stickers.
- Reasonable health and safety precautions should be taken when using a computer. The

Agreement Terms for any device loaned by LwLAT: Agreement for pupils and parents/carers	
Signed (pupil):	**Date:**
Parent/carer's agreement: I, the parent/carer, have read or had explained and understand the terms and conditions in the home loan agreement. I understand that by breaching the conditions the loan of the computer may be withdrawn by the Learning without Limits Academy Trust.	
Signed (parent/carer):	**Date:**
Printed name:	
Academy Name:	