AMBITIONS
Academies Trust

LeAF
Studio

Online Safety Policy

SCOPE:	Academy Policy
AUTHOR/ORIGINATOR:	Mrs N Lapskas
NAME OF RESPONSIBLE DIRECTOR/PRINCIPAL:	Mrs N Lapskas, Academy Principal & Mr J Webb, Sector Director
APPROVING COMMITTEE:	Sector Director
STATUTORY BASIS:	Non-Statutory Policy
REQUIREMENT TO PUBLISH ON WEBSITE:	No
DATE RATIFIED:	September 2020
DATE DISTRIBUTED TO STAFF:	September 2020

Outstanding Achievement for All

Online Safety Policy

Contents

Online Safety Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

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

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Mr JPhillips.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The Principal

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

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy safeguarding leads are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 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 school to the Principal and/or governing board

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

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 school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 (appendix 2).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

Through the school's Personal Development programme, pupils 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 a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

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

Cyber-bullying

Definition

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 the school's Anti-Bullying policy.)

Preventing and addressing cyber-bullying

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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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 through our Personal Development programme, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school 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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Behaviour for Learning policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if:

a) it involves illegal material

b) there is a serious threat to kill or harm another student

c) there has been harassment over a period of time

d) parents are becoming involved in sending abusive messages

and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School 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 pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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 school rules

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 school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them inside the school building during school time other than at the following times:

- During break and lunchtime, in the canteen and outside area only.
- During lessons and tutor time when specifically directed to do so by the teacher

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour for Learning policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities only.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour for Learning policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT system or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Training

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.

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).

The DSL and deputies 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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the Senior Leadership Team. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for Learning policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT Acceptable Use Policy

Appendix 1: Acceptable Use Agreement for KS4 and KS5 students and parents/carers

This agreement will help keep me safe and happy at school and home and help me to be fair to others.

1. I will treat myself and others with respect at all times; when I am online or using any device, I will treat everyone as if I were talking to them face to face.
2. Whenever I use a device, the internet or any apps, sites and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
3. I consider my online reputation with everything that I post or share – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
4. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling. I will remember the principles of the Digital 5 A Day.
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
7. If I see anything that shows people hurting themselves or encouraging others to do so, I will report it on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
9. I will only use the school's internet, systems, devices and logins for school-related activities for activities that are appropriate to what I am doing at that time (e.g. at school I don't play games unless I am allowed to, e.g. during lunch, and at home I don't access inappropriate sites or apps).
10. Whenever I use the internet or devices in school **OR use school devices at home OR log in on home devices at home**, I may be monitored or filtered; the same behaviour rules always apply.
11. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
12. I will not try to bypass school security in any way or access any hacking files or tools.
13. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
14. I will use the internet, apps, sites & games responsibly; I will not use any that are inappropriate for school use or for my age, including sites which encourage hate or discrimination.
15. I understand that any information I see online could be biased and misleading, so I should always check sources before sharing (see fakenews.lgfl.net for support).
16. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
17. I will not post, look at, up/download or share material that could be offensive, harmful or illegal. If I come across any, I will report it immediately.
18. I know some sites, games and apps have age restrictions (most social media are 13+) and I should respect this. 18-rated games are not more difficult but inappropriate for young people.
19. When I am at school, I will only message or mail people if it's relevant to my learning.

20. Messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
21. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will not open a file, hyperlink or any other attachment.
22. I will not download copyright-protected material (text, music, video etc.).
23. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
24. Livestreaming can be fun, but I always check my privacy settings and know who can see what and when. If I livestream, my parents/carers know about it.
25. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.
26. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
27. **When learning remotely, teachers and tutors will not behave any differently** to when we are in school. If I get asked or told anything that I would find strange in school, I will tell another teacher.
28. I will only use my personal devices (mobiles, smartwatches etc) in school if I have been given permission, and I will never take secret photos, videos or recordings of teachers or students, **including when learning remotely.**
29. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
30. Many apps can identify where I am or where I made a post or took a photo, so I know how to turn off location settings so everyone doesn't see where I am, where I live or go to school.
31. What I do on devices should never upset or hurt others & I shouldn't put myself or others at risk.
32. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
33. I don't have to keep a secret or do a dare or challenge just because someone (even a friend) tells me to – real friends don't put you under pressure to do things you don't want to.
34. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
35. I can always say no online, end a chat or block someone; if I do, it's best to talk to someone, too.
36. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get in touch with Childline, The Mix, or The Samaritans.

School name: ____LeAF Studio School__________________

Student's name: __________________________________ Year Group: __________

Student's signature: ______________________________ Date: ____/____/20____

Parent / carer name: ____

Parent's signature: ______________________________ Date: ____/____/20____

Appendix 2: ICT Acceptable Use Agreement (AUA) for Staff, Trainees, Volunteers, Members, Trustees and Academy Committee Members

All Staff, Trainees, Volunteers, Members, Trustees and Academy Committee Members with access to Ambitions Academy Trust (AAT) sites or computer devices, services and networks to sign an Acceptable Use Agreement (AUA), which outlines how we expect them to behave when using them, both in and out of academy.

This AUA is reviewed annually, and it is a requirement to sign it upon entry to the Trust and every time changes are made (usually also annually). **It is not exhaustive.**

All computer equipment, services and network access are intended to enhance professional activities, including teaching, research, administration and management. This agreement forms part of the Trust's ICT Acceptable Use Policy and has been drawn up to protect all parties - the students, the staff, the Academy and the Trust.

Agreeing to the terms of this agreement is a condition of use. Access to computer equipment, services and networks will form a condition of employment or engagement with Ambitions Academies Trust.

The Trust reserves the right to examine or delete any files that may be held on its computer systems or cloud services; or to monitor electronic communication and internet sites visited for the specific purpose of safeguarding.

I agree to the following terms:

a) Access to any device, network or cloud service must only be made via my authorised account and password, which must not be made available to any other person;

b) I will ensure the security of any device, network or cloud service I use, by locking devices with a password when unattended;

c) All internet use should be appropriate to professional activity or students' education;

d) Activity that threatens the integrity of the Trust's ICT systems, or that attacks or corrupts other systems, is forbidden;

e) Use of cloud and email services provided by the Trust for private interests, including personal financial gain, gambling, political purposes or advertising, is forbidden;

f) I am responsible for the email and instant messages I send and for adhering to the professionalism expected of all colleagues in our Email Policy;

g) When communicating electronically including the use of social media, I will behave in a positive manner, not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the Trust, Academy or teaching profession into disrepute. This applies both to public pages and to private posts;

h) Use of personal devices onsite, is controlled and any use should be limited and represents a consent to monitoring;

i) I must treat pupil data (including images of them, reports and safeguarding information) in strictest confidence and will not create, store or transmit it unless encrypted and viewable only by those with a legitimate professional reason, or as otherwise directed by the Data Protection Policy;

j) Appropriate images and videos of pupils and their work may be taken on a personal device in a group setting only by permanent staff, where parental consent for the purpose exists and an Academy device is not available, so long as they are deleted as soon as reasonable (including any automatic backups);

k) I will ensure in advance that any material I obtain or display from the internet to students is appropriate for the audience, especially when bypassing filtering, and necessary to an educational purpose;

l) Copyright of materials and intellectual property rights must be respected;

m) I understand that all activity using the Trust's devices, services and networks may be filtered and monitored without further warning.

n) If am allocated a device with specific permission to remove it from site, I will:

    i) Take reasonable care to protect it from data loss and physical loss or damage;
    ii) Be the sole user (not family) when offsite;
    iii) Only allow colleagues to use it with their own login;
    iv) Return it to the Trust Office or Academy when requested, after reasonable notice;
    v) Use it for professional purposes connected with education only;
    vi) Recognise that the device remains subject to routine monitoring;
    vii) Recognise that the device remains the property of the Trust at all times.

Academy name: ____

Full name: ____

Position: ____

Signed: ________________________________ Date: ____/____/20____

Please sign two copies of this Acceptable Use Agreement.

Return a copy to the Trust or Academy Administration Lead and retain a copy for your own record.

Appendix 3: Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**