ACORN MULTI ACADEMY TRUST

Online Safety Policy

Document control table			
Document Suite:	**Safeguarding**	**Document Title:**	Online Safety Policy
Document Type:	Policy	**Version number:**	v1
Author (Job title):		Network/ICT Manager	
Staff responsibility: (name or post)		Network Manager	
Source		Internal	
Date adopted	31st March 2022	**Formal Approval by:**	Trust Board
Review information:	***Scheduled***	***Next Review Due By***	
Formal Approval	Every two years	**March 2024**	
This policy should be read in conjunction with: Child protection and Safeguarding Dealing with allegations of abuse made against a child or young person Managing allegations against staff and volunteers Code of conduct for staff and volunteers and Social Media Policy		Acceptable Use Policies for staff, pupils and others Procedures for logging and responding to concerns about a child or young person's wellbeing Behaviour & Anti-bullying policy and procedures Photography and image sharing guidance Remote learning	

Document History			
Version	***Date***	***Reviewer***	***Note of revisions***
v1	18/03/2022	Clerk	

Contents

1 Purpose, scope and aims 3
2 Legal framework and Updates 4
3 Responsibilities 4
4 Procedures 5
5 Curriculum 6
6 Staff Training 6
7 Access to the MAT's Technology 7
8 Dealing with Misuse 7
9 Responding to Abuse 8
10 Monitoring and review 8

1 Purpose, scope and aims

Acorn Multi Academy Trust and its individual Academies are committed to promoting and safeguarding the welfare of all pupils and an effective online safety strategy is paramount to this.

This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation happen through the online medium, and anti-bullying, as an increasing level of bullying also takes place through the online medium.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices including protecting the whole MAT community from illegal, inappropriate and harmful content or contact
- establish effective mechanisms to identify, intervene and escalate incidents where appropriate

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Acorn MAT's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

In considering the scope of these online safety procedures, we take a wide approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology). This policy applies to all members of the MAT community, including staff and volunteers, pupils, parents and visitors, who have access to Academy Technology whether on or off our premises, or otherwise use Technology in a way which affects the welfare of other pupils or any member of the MAT community or where the culture or reputation of the MAT is put at risk.

This policy should be read alongside Acorn Multi Academy Trust and individual Academy policies and procedures on:
Child protection and Safeguarding
Dealing with allegations of abuse made against a child or young person

Managing allegations against staff and volunteers
Code of conduct for staff and volunteers and Social Media policy
Acceptable Use Policies for staff, pupils and others
Procedures for logging and responding to concerns about a child or young person's wellbeing
Anti-bullying policy and procedures
Photography and image sharing guidance
Remote learning

2 Legal framework and Updates

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
child protection learning.nspcc.org.uk/child-protection-system

There are a number of new risks mentioned in Keeping Children Safe In Education 2021, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk of pupils missing opportunities to disclose such abuse during the lockdowns or periods of absence.

Following the government's investigation into peer-on-peer sexual abuse and Ofsted review, we have reviewed this policy to ensure that sufficient safeguards and processes are in place to allow pupils to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately – we ensure pupils are aware of the new NSPCC helpline and have reviewed our internal reporting channels.

We stay up to date with the latest news, risks, opportunities, best-practice and trends through Local Authority safeguarding updates and audits such as the SWGfL 360.

3 Responsibilities

Directors and governors, particularly those with a designated safeguarding role, work with Heads of School and DSLs (which may be the same person) to ensure this policy is updated, implemented and monitored effectively. They work with the Network/IT team within the MAT and staff with designated responsibilities for supporting IT in each Academy to ensure that staff, children, volunteers and others are supported and trained in order to achieve the aims of the policy.

3.1 Network/IT Team

The IT Team are responsible for the effective operation of the filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using any area of the Trust's network.

The IT Team is responsible for ensuring that:

- the MAT's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
- the user may only use the MAT's Technology if they are properly authenticated and authorised;
- the MAT has an effective filtering policy in place and that it is applied and updated on a regular basis;
- the risks of pupils and staff circumventing the safeguards put in place by the MAT are minimised;
- the use of the MAT's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation;
- monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the MAT's network

The IT Team will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

The IT Lead will report regularly to the SLT on the operation of the MAT's Technology. If the IT Lead has concerns about the functionality, effectiveness, suitability or use of Technology within any Academy, he will escalate those concerns promptly to the Head of School.
The IT Team is responsible for bringing any matters of safeguarding concern to the attention of the appropriate DSL in accordance with Child Protection & Safeguarding Policy and Procedures.

4 Procedures

We will seek to keep children and young people safe by:
appointing an online safety coordinator, which for each Academy may or may not be the same person as the Designated Safeguarding Lead
providing clear and specific directions to staff and volunteers on how to behave online through our code of conduct and acceptable use policies for adults
supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
supporting and encouraging parents and carers to do what they can to keep their children safe online
developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
reviewing and updating the security of our information systems regularly
ensuring that usernames, logins, email accounts and passwords are used effectively
ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
providing supervision, support and training for staff and volunteers about online safety

examining and risk assessing any social media platforms and new technologies before they are used within the organisation

5 Curriculum

The safe use of Technology is integral to the School's computing curriculum. pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS as children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment; children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching pupils:

- about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying, radicalisation and extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

The MAT's Acceptable Use of Technology agreement for pupils (completed online annually) sets out the rules about the use of Technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using Technology. pupils are reminded of the importance of this policy on a regular basis.

6 Staff Training

The MAT provides training on the safe use of Technology to staff so that they are aware of how to protect pupils and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur. Training materials are made available through the staff portal in the form of user guides and video tutorials.

Staff are regularly asked to review and sign up to the Acceptable Use of Technology Policy for Staff which gives clear guidance on Email & Internet Policy and Professional Use of Social Media.

Ongoing staff development training includes regular updates on Technology safety together with specific safeguarding issues including cyberbullying and radicalisation and training for all staff and volunteers on dealing with all forms of abuse, including emotional abuse, sexting, sexual abuse and sexual exploitation. Staff also receive data protection guidance on induction and at regular intervals afterwards. The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the MAT's overarching approach to safeguarding.

7 Access to the MAT's Technology

The MAT provides internet access and an email system to pupils and staff as well as other Technology. pupils and staff must comply with the respective Acceptable Use of Technology Policies when using School Technology. All such use can be monitored by the IT Team.

Pupils and staff have individual usernames and passwords to access the MAT cloud-based data and our email system and these must not be disclosed to any other person. Any student or member of staff who has a problem with their usernames or passwords must report it to the IT Team immediately.

Any laptop, tablet or other mobile electronic device must be connected to the appropriate WiFi network. Each Academy has a separate Wi-Fi connection available for use by visitors as well as for pupils. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service can be monitored by the IT Team.

Use of mobile electronic devices

The School has appropriate filtering and monitoring systems in place to protect pupils using the Internet (including email text messaging and social media sites) when connected to our own WiFi network. Mobile devices equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. Since the MAT cannot put adequate protection for the pupils in place, pupils are not allowed to use their mobile devices to connect to the Internet including accessing email, text messages or social media sites when in our care.
The School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Pupils. The use of mobile electronic devices by staff is covered in the Acceptable Use of Technology Policy for Staff.

Unless otherwise agreed, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency. The School's policies apply to the use of Technology by staff and pupils whether on or off MAT premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the MAT community or where the culture or reputation of the MAT is put at risk.

8 Dealing with Misuse

Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the Academy in accordance with this policy and the Academy's safeguarding and disciplinary policies and procedures.

Misuse by pupils

Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying. Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy).

Misuse by staff

Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures. If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy and Managing Allegations Policy.

Misuse by any user

Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of School or the IT Team. The MAT reserves the right to withdraw access to their networks by any user at any time and to report suspected illegal activity to the police. If the MAT considers that any person is vulnerable to radicalisation they will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

9 Responding to Abuse

If online abuse occurs, we will respond to it by:

- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term

10 Monitoring and review

All serious incidents involving the use of Technology will be logged with the relevant Head of School and/or DSL.

The implementation and review of this policy will be undertaken at least annually and/or in response to any serious incident, and will consider the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the MAT are adequate.

Consideration of the effectiveness of the MAT's online safety procedures and the education of pupils about keeping safe online will be included in the annual reviews of safeguarding.