Academy 1 Sports Ltd

ONLINE SAFETY POLICY

Policy Statement

Academy1 group works with children and learners plus as part of our delivery and provision.

Ensure the safety and wellbeing of all children and learners is paramount when they are using the internet, social media or mobile devices.

Ensure that as an organisation we operate in line with values and within the law in terms of how we use online devices.

Legal Frameworks

Keeping children safe in Education (Revised version) 2022.

Data Protection Act 2018.

We believe that:

Children and learners should never experience abuse of any kind, and this includes:

- Access to illegal, harmful, or inappropriate images or other content.
- Grooming by those with whom they make contact on the internet where the theme could be radicalization or Extremism or viewing any inappropriate images.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Online-bullying.
- Access to unsuitable video / internet games.

Children and young people should be able to use the internet for education and personal development and where possible avoid:

- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- Hacking, viruses, and system security.
- The potential for excessive use may impact on children's social and emotional development and learning.

Abuse

When defining “abuse”:

“Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults, or another child or children.”

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content:

Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact:

Being subjected to harmful online interaction with other users; for example: 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: Online behaviour that increases the likelihood of, or causes, harm; for example, 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.

Commerce: - Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

As with all other risks, it is difficult to eliminate the risks completely. By providing good examples/role models and by raising awareness, it is possible to build resilience for learners, so that they have the confidence and skills to deal with these risks.

Responsibility

- Our organisation has a significant role to play in keeping children, learners, and staff safe and that includes online. Whether we provide internet access or not, children/learners will usually have access to the internet at home and we need to ensure their safety and well-being wherever they are.
- Children / learners who are using the internet, social media, or mobile phones in a way that shows respect for others.
- Ensuring that images of children / learners are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Ensuring personal information about children / learners who are involved in our organisation is held securely and shared only as appropriate.
- Obtaining additional support and where to report issues.
- Raise awareness in relation to keeping safe online where appropriate.

- We know and record what personal data we hold, where this data is held, why and which member of staff/volunteer has responsibility for managing it.
- Gain consent to obtain, store and process personal data from families, staff and volunteers and identify the more sensitive information classed as special category data.
- Will hold only the minimum personal data necessary to enable us to perform our function and will not hold that data for longer than necessary for the purposes for which it was collected.
- We look after staff / learner information about how we look after their data and what their rights are in a clear Privacy Notice.
- Ensure procedures are in place to deal with the individual rights of the data subject, e.g. subject access requests.
- Ensures that personal data stored on a mobile device or removable media encrypted and password protected and is securely deleted from devices when no longer in use.
- Staff use the electronic equipment that they have been issued sensibly, this is part of the joiner information that we access on the laptop and stored internally.
- Understand and follow the procedures for reporting and recording online safety.
- Digital communications are transparent, open to scrutiny and conducted using systems agreed by the organisation.

Online delivery

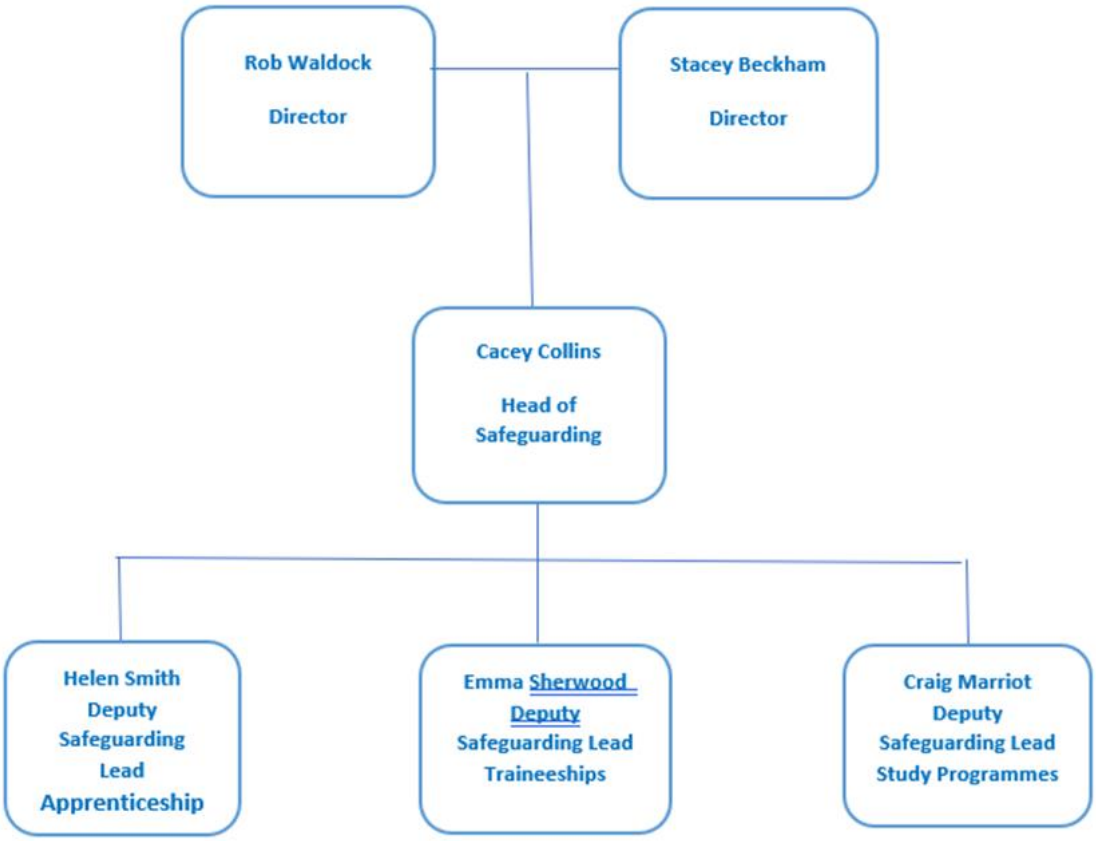
Children/Young People/Learners:

- To ensure that they abide and behave appropriately in relation to any online delivery sessions.
- Should demonstrate positive online behaviour, to be on time when they are logging in and show mutual respect and tolerance to other participants.

Safeguarding

- Responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/procedures.
- Where possible offers advice and support for all children / learners.
- Raise awareness of any issues relating to Online safety to staff.
- Consults with any national/local organisation (as relevant).
- Act on any concerns raised on 'My concerns' in relation to Online safety.

Safeguarding Structure



Name	Contact number	Email address.
Rob Waldock	7739487332	Robwaldock@academy1group.com
Stacey Beckham	7598526707	Staceybeckham@academy1group.com
Cacey Collins	795220452	Caceycollins@academy1group.com
Helen Smith	7908493122	Helensmith@academy1group.com
Emma Sherwood	7983870552	Emmasherwood@academy1group.com
Cacey Marriot	7980716109	Caceymarriot@academy1group.com

Head Safeguarding & Prevent Officer (Cacey Collins)

Should you have concerns in relation to radicalisation they should immediately be referred to the Prevent Lead. The Prevent Lead is responsible for making any further referrals thereon (i.e. Channel).

Provide information on counselling if required for staff members affected by abuse or disclosure of abuse.

Designated Safeguarding Lead for Study Programme (Craig Marriott)

In the absence of the Head Safeguarding Officer, the deputy will be the main point of contact.

Designated Safeguarding Lead for Apprenticeships (Helen Smith)

In the absence of the Head Safeguarding Officer, the deputy will be the main point of contact.

Designated Safeguarding Lead for Traineeships (Emma Sherwood)

In the absence of the Head Safeguarding Officer, the deputy will be the main point of contact.

Personal Data

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, organisations are likely to be subject to greater scrutiny in their care and use of personal data. Under UK law, the Data Protection Acts set out the way you should use and keep personal data. The Information Commissioner's Office (ICO) regulates data protection in the UK. Any organisation that uses or keeps personal data must comply with that law.

Personal data in our organisation is recorded, processed, transferred, and made available according to the current data protection legislation.

Ensure staff:

- Take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a breach, understand the need for urgency and know who to report it to within the setting.
- Will not transfer any setting personal data to personal devices.

Where we suspect that misuse might have taken place, but that the misuse is not illegal, we will investigate, preserve evidence, and protect those conducting the investigation.

Incidents of misuse by staff will be dealt with through agreed disciplinary procedures.

Technology

Devices

Technology is a part of day-to-day operations in our organisation and is used in many valuable ways to contribute to the work of our setting. We use:

- Administrative computers.
- Mobile phones.
- Laptops.

We monitor the use of these devices and how they are used through:

- Supervision.
- Technical monitoring.

We issue clear guidance for staff as on the use of personal mobile devices within our setting through:

Clear acceptable use policy.

Clear rules and guidance for visitors on the use of personal mobile devices within our organisation.

Security of equipment

Our organisation has effective systems in place to ensure the security of devices, systems, images, and personal devices. These are regularly reviewed and updated, in the light of constantly changing technology and new online security threats.

Having the latest operating system security updates installed.

Regularly updated antivirus and malware protection on all devices.

Protection from theft, loss, or physical attack.

Data being regularly and securely backed up and stored off-site or on a secure cloud service.

Any removable media containing personal or sensitive data (e.g. USB sticks or devices that leave our setting) is secured through password and/or encryption.

All official organisation devices and networks can only be accessed through secure passwords assigned to individual appropriate users. This allows us to manage and identify who has access to our systems.

Ensured staff only have access to appropriate agreed content on our systems through appropriate access and filtering.

Effective monitoring in place to alert us to any illegal access or misuse of our systems.

Digital Images.

Social Media and Communications.

Our organisation uses a range of online services to communicate with our community, which include:

- Website
- Social media pages
- Social media messaging
- Text messaging
- Online portal pages
- Closed messaging systems.
- Email

Appendix – Additional Guidance

Links to other organisations or documents

The following links may help those who are developing or reviewing a setting online safety policy and creating their online safety provision:

- UK Safer Internet Centre
- Safer Internet Centre – https://www.saferinternet.org.uk/
- Childnet – http://www.childnet-int.org/
- Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
- Internet Watch Foundation - https://www.iwf.org.uk/
- Report Harmful Content - https://reportharmfulcontent.com/

Other

- CEOP - http://ceop.police.uk/
- PREVENT - Prevent duty guidance for England, Scotland, and Wales
- Safer Recruitment Consortium - Guidance for safer working practice for adults that work with children and young people -
- Online Safety BOOST – https://boost.swgfl.org.uk/
- Educating learners
- SWGfL Evolve - https://projectevolve.co.uk
- UKCIS – Education for a connected world framework

- Childnet - Digital well-being - guidance for parents
- UKSIC Safer Internet Day
- ThinkUKnow - https://www.thinkuknow.co.uk/

Legislation

Organisations should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

- Computer Misuse Act 1990
- This Act makes it an offence to:
- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities.

Maliciously corrupt or erase data or programs.

- Deny access to authorised users.
- Data Protection Act 1998
- This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.
- The Data Protection Act 2018:

.

This Policy will be reviewed annually and/or in accordance with legislative updates. It was last reviewed on 4th October 2022 and will be reviewed next on 4th October 2023

Signed: 

Printed Name: D. Blackburn

Role: Quality Team

Date: Oct 22