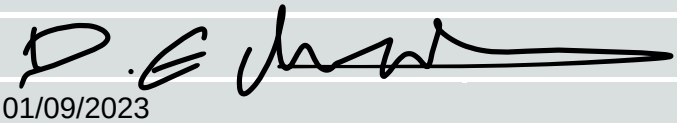
Marshall Skills Academy Online Safety Policy

Approved by:	Dan Edwards	**Date:**	01/10/2023
Signature:			
Last reviewed on:	01/09/2023		
Next review due by:	01/09/2023		

Contents

1. Aims

1.1 The Marshall Skills Academy (MSA) aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and visitors
- Identify and support groups of learners that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole MSA 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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

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

2. Legislation and guidance

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

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

It also refers to the DfE'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.

3. Roles and responsibilities

3.1 The Head of Capability (HoC)

3.1.1 The HoC has overall responsibility for monitoring this policy and holding the General Manager to account for its implementation.

3.1.2 The HoC will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.1.3 The HoC will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard learners.

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

3.1.5 The Welfare Team should ensure learners at the MSA are taught how to keep themselves and others safe, including keeping safe online.

3.1.6 The HoC must ensure the MSA has appropriate filtering and monitoring systems in place on any MSA devices and networks and will regularly review their effectiveness. The SLT will review the DfE filtering and monitoring standards, and discuss with Head of Operations and service providers what needs to be done to support the MSA in meeting these standards, which include (though not exhaustive):

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Head of Operations will assist and oversees online safety

3.1.7 MSA staff will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable adults, children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all learners in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The General Manager (GM)

3.2.1 The GM is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the MSA.

3.3 The designated safeguarding lead (DSL)

3.3.1 Details of the MSA DSL and Welfare Officers are set out in our safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety of learners in the MSA, in particular:

- Supporting the GM in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the GM and HoC to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on Marshall Skills Academy devices and networks

- Working with the Head of Operations to make sure the appropriate systems and processes are in place
- Working with the GM, Head of Operations and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the MSA Safeguarding policy
- Ensuring that any online safety incidents are logged 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 MSA Code of Conduct
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the MSA to the GM and/or HoC
- Undertaking annual risk assessments that consider and reflect the risks learners face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Head of Operations

3.4.1 The Head of Operations is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on MSA devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at the MSA, including access to terrorist and extremist material
- Ensuring that the MSA 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 MSA ICT systems on a weekly 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 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the MSA Code of Conduct

  This list is not intended to be exhaustive.

3.5 All staff and volunteers

3.5.1 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 MSA ICT systems and the internet, and ensuring that learners follow the MSA terms of acceptable use and as defined in the Marshall ICT Acceptable Use Policy

- Knowing that the Head of Operations is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by immediately notifying the DSL and General Manager
- Following the correct procedures by issuing a request to deviate in writing to the Head of Operations if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the MSA Code of Conduct
- 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'

This list is not intended to be exhaustive.

3.6 Parents/carers of learners under the age of 18

3.6.1 Parents/carers are expected to:

- Notify a member of staff or the GM of any concerns or queries regarding this policy
- Ensure their child understands and agrees to the terms on acceptable use of the MSA ICT systems and internet
- Parents/carers can seek further guidance on keeping children 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

3.7 Visitors and members of the community

3.7.1 Visitors and members of the community who use the MSA 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.

4. Educating learners about online safety

4.1 Learners will be taught about online safety as part of the apprenticeship curriculum:

4.1.2 During the apprenticeship learners may be reminded:

- Of 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 that 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)

The safe use of social media and the use of social medial for business will also be covered where relevant.

5. Cyber-bullying

5.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power.

5.2 Preventing and addressing cyber-bullying

5.2.1 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.

5.2.2 The MSA Welfare Team will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

5.2.3 All staff 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).

5.2.4 The MSA may send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children or learners who may be affected.

5.2.5 In relation to a specific incident of cyber-bullying, the MSA will follow the processes set out in the Code of Conduct. Where illegal, inappropriate, or harmful material has been spread among pupils, the MSA will use all reasonable endeavours to ensure the incident is contained.

5.2.6 The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6. Examining electronic devices

The GM, and any member of staff authorised to do so by the GM can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Content that could / does pose a risk to staff or other learners, and/or
- Is identified in the MSA Code of Conduct as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence(s)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from GM and DSL
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the learner's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the MSA or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and / or GM to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child/learner(also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

7. Acceptable use of the internet in the MSA

7.1 All learners, staff, volunteers and visitors are expected to sign an agreement regarding the acceptable use of the MSA ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the MSA terms on acceptable use if relevant.

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

7.1.2 We will monitor the websites visited by pupils, staff, volunteers, and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices at Marshall Skills Academy

8.1 Learners may bring mobile devices into the MSA, but are not permitted to use them during:

- Lessons (theory or practical unless approved by the trainer)

8.1.2 Any use of mobile devices in the MSA by learners must be in line with the acceptable use agreement

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the MSA code of conduct and Marshall policies, which may also result in the confiscation of their device.

9. Staff using work devices outside of the Marshall Skills Academy

Refer to Marshall Acceptable Use of IT Policy

10. How the MSA will respond to issues of misuse

10.1 Where a learner misuses the MSA ICT systems or internet, we will follow the procedures set out in our capability and code of conduct policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.1.1 Where a staff member misuses the MSA ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Marshall HR Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

11.1 All new staff members of the MSA 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.

11.1.2 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).

11.1.3 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 children are especially 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

11.1.4 The DSL and Welfare Officers 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.

11.1.5 Senior Leaders and support staff at the MSA will also receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

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

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

12. Monitoring arrangements

12.1 The DSL and Welfare Officers log behaviour and safeguarding issues related to online safety.

12.2 This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Head of Capability. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Code of Conduct policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy