Online Safety Policy

MK Christian Foundation

Approved by:	Board of Trustees	**Date:**	November 2024
Last reviewed on:	November 2024		
Next review due by:	November 2025		

Contents

1. Aims

MK Christian Foundation aims to:

- Have robust processes in place to ensure the online safety of trainees, staff, volunteers and board members
- Identify and support groups of trainees 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
- 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.

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 educators stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on trainees' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement.

3. Roles and responsibilities

3.1 The board of trustees

The board of trustees has overall responsibility for monitoring this policy and holding the Head of Learning and Director to account for its implementation.

The board of trustees 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.

The board of trustees should ensure trainees are taught how to keep themselves and others safe, including keeping safe online.

The board of trustees must ensure the organisation has appropriate filtering and monitoring systems in place on devices and networks, and will regularly review their effectiveness. This includes:

- 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 safeguarding needs.

All board members will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the organisation's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-provision approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable trainees, victims of abuse and some trainees 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 trainees in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Head of Learning and Director

The Head of Learning and Director are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation.

3.3 The designated safeguarding lead

Details of the organisation's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety at MK Christian Foundation, in particular:

- Supporting the Head of Learning and Director in ensuring that staff understand this policy and that it is being implemented consistently throughout the organisation
- Working with the Head of Learning and board of trustees 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 devices and networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Head of Learning, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the organisation's child protection 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 behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- 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

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure trainees are kept safe from potentially harmful and inappropriate content and contact online, including terrorist and extremist material
- Ensuring that the organisation's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- 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 behaviour policy

3.5 All staff and volunteers

All 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 ICT systems and the internet (appendix 3), and ensuring that trainees follow the terms on acceptable use
- Knowing that the DSL 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 contacting the safeguarding team via email (safeguarding@mkchristianfoundation.co.uk)
- 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 behaviour policy

- 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'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of Learning of any concerns or queries regarding this policy

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

Visitors and members of the community who use the organisation'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.

4. Educating trainees about online safety

Trainees will be taught about online safety as part of our enrichment, employability and progression (EEP) strand of the curriculum:

Trainees will be taught:

- To understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- To recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- 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)

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable trainees, victims of abuse and some trainees with SEND.

5. Working with parents and carers

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

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

6. Cyber-bullying

6.1 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. (See also the behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

Cyber bullying will be actively discussed with trainees as part of our EEP curriculum, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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

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.

6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, trainees and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. We currently do not use any AI tools in the delivery of our education programme but, if we were to look at developing our programme to include the use of AI, appropriate training around the risks will be provided and risk assessments will be put in place.

MKCF recognises that AI has the potential to be used to bully others. For example, in the form of ‘deepfakes’, where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone’s likeness.

MKCF will treat any use of AI to bully others in line with our anti-bullying/behaviour policy.

7. Acceptable use of the internet

Use of the organisation’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 trainees, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Trainees using mobile devices

Trainees may bring mobile devices to MK Christian Foundation, but are not permitted to use them during:

- Functional Skills and other learning sessions
- Working hours on social enterprise

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

9. Staff using work devices outside of the organisation

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Work devices must be used solely for work activities.

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

10. How the organisation will respond to issues of misuse

Where a trainee misuses the ICT systems or internet, we will follow the procedures set out in our behaviour policies. 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 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 staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training 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.

Trustees 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the board of trustees.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy

- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure