OMNIA
FOUNDATION

DIGITAL SAFETY POLICY

Policy type	Statutory
Review period	Biennial
Last reviewed on	Spring 2023
Next review due	Spring 2025
Approval level	Chief Operating Officer
Approved by (Name, date, signature)	E.V.Keeble
Executive Board, 22nd February 2023	
Chief Operating Officer, Liz Keeble	
Published on	Omnia Foundation Website

POLICY FOR FACEBOOK PAGE

Mission

We believe in investing in people. As professionals in the teaching and training professions, we strive to provide a better future for the children, young people and home settings we work with. Success for us means unleashing the potential of each individual so they can grow, develop and reach the potential of which they are capable. Our values are grounded in our determination to be the change we want to see in the world, through passion, commitment and integrity. We strive to plant a seed of kindness and compassion in a generation that will produce resilience and hope and enable them to aspire and achieve productive and fulfilled lives. Our success is measured in the lives we changed.

At the Omnia Foundation, we create a secure and safe environment that encourages communication, self-belief, mutual respect and success. We provide a rich and balanced curriculum that develops every child, allowing them to achieve their true potential.

Aims of the policy

The Omnia Foundation aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and directors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole foundation 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, anti-Semitism, 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 scam

Legislation and guidance

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for educational establishments. It also complies with the following:

- Teaching Online Safety In Schools
- Harmful Online Challenges and Online Hoaxes
- Online Abuse and Bullying Prevention Guide
- Sharing Nudes and Semi-Nudes
- Protecting children from radicalisation - The Prevent Duty

Educational establishments should be aware as far as possible of the possible online threats to student safety, as part of their wider safeguarding responsibilities. Educational settings should consider how they teach students to keep themselves safe online and pay particular attention to the list below:

- online bullying and associated mental health and wellbeing;
- the security of personal information;
- device addiction;
- gaming addiction;
- exploitation;
- grooming;
- accessing inappropriate material;
- sharing of inappropriate material;
- significant risk of harm / actual harm.

Educational establishments cannot eradicate the risks that are associated with internet use but by providing students and homes settings with information on how to practise online safety they can help to mitigate the risks and help to keep students safe from harm.

This policy should also be read in conjunction with the Me, Myself and I Policy, Rights & Responsibilities Policy, Child Protection Policy, Anti-Bullying Policy and Screen and Search Policy

Roles and responsibilities

The Executive Board

The Executive Board has overall responsibility for monitoring this policy and holding the Head of Foundation to account for its implementation.

The Executive Board will coordinate regular meetings with appropriate staff to discuss digital safety, and monitor safety logs as provided by the designated safeguarding lead (DSL).

All directors will:

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

The Head of Foundation

The Head of Foundation is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the foundation.

The designated safeguarding lead

Details of the foundation's DSL and the deputies are set out in our Child Protection policy as well as relevant job descriptions.

The DSL and Deputies takes lead responsibility for digital safety in school, in particular, where the Head of Foundation is not the DSL:

- Supporting the Head of Foundation in ensuring that staff understand this policy and that it is being implemented consistently throughout the foundation
- Working with the Head of Foundation, ICT manager and other staff, as necessary, to address any digital safety issues or incidents
- Ensuring that any digital safety incidents are logged on CPOMs 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 foundation's Rights & Responsibilities Policy
- Updating and delivering staff training on digital safety (appendix 3 contains a self-audit for staff on digital safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on digital safety in the foundation to the Head of Foundation and/or Executive Board

This list is not intended to be exhaustive.

The Digital Systems manager

The Digital Systems manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate digital content and contact while on site, including terrorist and extremist material
- Ensuring that the foundation's digital 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 foundation's digital systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any digital safety incidents are logged on CPOMS 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 foundation's digital systems and the internet (appendix 2), and ensuring that students follow the foundation's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any digital safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the foundation's Rights & Responsibilities Policy.

This list is not intended to be exhaustive.

Home Settings

Home settings are expected to:

- Notify a member of staff or the Head of Foundation of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the foundation's digital systems and internet (appendices 1)

Home settings 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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the foundation's digital 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 students about digital safety

Students will be taught about digital safety as part of the curriculum. This forms part of the Me, Myself & I programme of study which addresses Relationships, Sex and Health Education as well as Personal and Social education.

By the end of their time in the Omnia Foundation students will understand:

- Their rights, responsibilities and opportunities online, including that the same expectations of their choices apply in all contexts, including on digital platforms
- About digital risks, including that any material someone provides to another has the potential to be shared digitally, creates a digital footprint and the subsequent 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 react and respond to sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including prison sentences
- 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

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

Educating homes settings about online safety

The foundation will raise home settings' awareness of digital safety in letters or other communications and in information via our website. This policy will also be shared with home settings.

Digital safety will also be covered during contact visits with home settings.

If home settings have any queries or concerns in relation to digital safety, these should be raised in the first instance with the Head of Foundation and/or the DSL.

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

Cyber-bullying

Definition

Cyber-bullying takes place on digital platforms, 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. Further details can be found in the foundation's Anti-Bullying Policy and Rights & Responsibilities Policy.

Preventing and addressing cyber-bullying

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

The foundation's curricular programme will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All 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, and other subjects where appropriate.

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

The foundation also sends information/leaflets on cyber-bullying to home settings 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 foundation will follow the processes set out in the foundation's Anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among students, the foundation 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 it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

Foundation 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 students' 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 learning

If inappropriate material is found on the device, in line with our Screen and Search Policy, it is the decision of the Head of Foundation or member of SLT to:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the foundation's screen and search policy

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

Acceptable use of the internet on-site

All students, representatives of home settings, staff, volunteers and directors are expected to sign an agreement regarding the acceptable use of the foundation's digital systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the foundationl's terms on acceptable use if relevant.

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

The websites visited by students, staff, volunteers, directors and visitors (where relevant) will be monitored regularly to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Students using mobile devices in school

Students' mobile phones are handled in accordance with the foundation's mobile phone charter which was agreed with students in Autumn 2021.

Staff using work devices outside working hours and off-site

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

In line with General Data Protection Regulations 2018 (GDPR), 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 off-site. Any USB devices containing data relating to the foundation must be encrypted. All devices must be stored securely, for example, if devices must be left in a vehicle, they should be kept in the boot where they are not visible.

If staff have any concerns over the security of their device, they must seek advice from the digital systems manager. Work devices must be used solely for work activities.

How the foundation will respond to issues of misuse

Where a student misuses the foundation's digital systems or internet, 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 foundation's digital 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The foundation 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 Level 2 training, as part of their induction, on safe internet use and digital 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).

- 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 at risk of abuse on digital platforms
- Children 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 abuse on digital platforms
- develop the ability to ensure students can recognise dangers and risks of activity on digital platforms and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake Level 3 child protection training, which will include digital safety, at least every 2 years. They will also update their knowledge and skills on the subject of digital safety at regular intervals, and at least annually.

Directors 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 Policy

Monitoring arrangements

Staff log behaviour and safeguarding issues related to digital safety on CPOMS and DSL will investigate and report according with safeguarding policy and procedures.

This policy will be reviewed every year by the Chief Operations Officer. At every review, the policy will be shared with the Executive Board.

Appendix 1: acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE OMNIA FOUNDATION'S DIGITAL SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND HOME SETTINGS

Name of student:

I will read and follow the acceptable use agreement policy

When I use the foundation's digital systems (like computers) and get onto the internet whilst on-site I will:

- Always use the foundation's digital systems and the internet responsibly and for educational purposes only
- Only use them when a member of staff is present, or with staff's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my hub staff team or from my home setting
- Tell a responsible adult immediately if I find any material which might distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a member of staff
- Use any inappropriate language when communicating online, including in emails
- Log in to the foundation's network using someone else's details
- Arrange to meet anyone offline without first consulting a responsible adult in my home setting, or without adult supervision

If I bring a personal mobile phone or other personal electronic device on-site:

- It will be handled in accordance with the Mobile Phone Charter

I agree that the foundation will monitor the websites I visit and that there will be consequences if I ignore this policy.

Signed (student):

Date:

Home settings agreement: I agree that my child can use the foundation's digital systems and internet when appropriately supervised by a member of foundation staff. I agree to the conditions set out above for students using the foundation's digital systems and internet, and for using personal electronic devices on-site, and will make sure my child understands these.

Signed (responsible adult from the home setting):

Date:

Appendix 2: acceptable use agreement (staff, directors, volunteers and visitors)

ACCEPTABLE USE OF THE FOUNDATION'S DIGITAL SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, DIRECTORS, VOLUNTEERS AND VISITORS

Name of staff member/director/volunteer/visitor:

When using the foundation's digital systems and accessing the internet on-site, or outside working hours off-site on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the foundation's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the foundation's network
- Share my password with others or log in to the foundation's network using someone else's details
- Take images of students without checking with staff first
- Share confidential information about the foundation, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the foundation

I will only use the foundation's digital systems and access the internet on-site, or outside working hours off-site on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the foundation will monitor the websites I visit and my use of the foundation's digital facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them off-site, and keep all data securely stored in accordance with this policy and the foundation's data protection policy.

I will let the designated safeguarding lead (DSL) and digital systems manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the foundation's digital systems and internet responsibly, and ensure that students in my care do so too

Signed (staff member/director/volunteer/visitor):

Date:

Appendix 3: digital safety training needs – self audit for staff

DIGITAL SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer: ____________________

Date: ____________________

Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for digital safety in the organisation?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the foundation's acceptable use agreement for staff, volunteers, directors and visitors?	
Are you familiar with the foundation's acceptable use agreement for students and home settings?	
Do you regularly change your password for accessing the foundation's digital systems?	
Are you familiar with the foundation's approach to tackling cyber-bullying?	
Are there any areas of digital safety in which you would like training/further training?	