# Online Safety Policy 2024

| | | |
|---|---|---|
| **Approved by:** | Safeguarding Committee | **Date:** 26th September 2024 |
| **Last reviewed on:** | 5th August 2024 | |
| **Next review due by:** | 5th August 2025 | |

| Document Control | | | |
|---|---|---|---|
| **Version** | **Author** | **Date** | **Changes/Updates** |
| V1 | Helen Kain | 26.06.23 | Policy written by HK<br>**Approved by the Board of Trustees – 28.06.23** |
| V2 | Helen Kain | 05.08.24 | Summary added at start of policy<br>**Approved by Safeguarding Committee – 26.09.24** |
| | | | |
| | | | |

**Summary of Online Safety Policy 2024**

**Purpose:**
Camphill Wakefield's Online Safety Policy ensures the protection and education of students, staff, volunteers, and trustees in the use of technology, including mobile phones and tablets. It establishes clear mechanisms to identify, intervene, and escalate incidents as needed.

**Key Categories of Risk:**
Content: Exposure to harmful content (e.g., pornography, fake news, racism).
Contact: Harmful interactions (e.g., grooming, peer pressure).
Conduct: Harmful personal online behaviour (e.g., cyberbullying).
Commerce: Risks like online gambling and phishing scams.
Legislation and Guidance:
Based on DfE's statutory guidance and includes the Education Act, Equality Act, and others.

**Roles and Responsibilities:**
Trustee Board: Oversees policy implementation and monitors online safety logs.
Chief Executive Officer (CEO): Ensures consistent policy implementation.
Designated Safeguarding Lead (DSL): Manages online safety issues and incidents, logs incidents, updates staff training, and liaises with external agencies.
External IT Organisation: Ensures security protection, updates safety mechanisms, and monitors IT systems.
All Staff and Volunteers: Understand and implement the policy, report incidents, and respond to online and offline safety concerns.
Parents/Carers: Notify staff of concerns and understand acceptable use terms.

**Education on Online Safety:**
Students are taught about online safety through tailored curriculum methods, recognising inappropriate content, protecting online identity, reporting concerns, understanding online risks, and more. Parents are informed through communications and provided with guidance on keeping children safe online.

**Preventing and Addressing Cyber-bullying:**
Includes educating students, staff, and parents on recognising and reporting cyber-bullying, following the Behaviour Policy, and involving external services if necessary.

**Examining Electronic Devices:**
Senior staff can search and delete inappropriate material on student devices if necessary. Complaints about this process are managed through the complaints procedure.

**Acceptable Use:**
Internet use at Camphill is for educational purposes only. Students may bring mobile devices but must store them during sessions. Staff must ensure the security of work devices used off-site.

**Misuse Management:**
Misuse of IT systems is addressed through behaviour policies and IT acceptable use terms. Serious incidents may be reported to the police.

**Training:**
New staff receive training on safe internet use and online safeguarding issues, with annual refreshers. The DSL and deputies undergo training every two years and regularly update their knowledge.

**Monitoring and Review:**
The DSL logs issues related to online safety. The DSL and Lead Trustee review the policy for safeguarding annually, considering the evolving risks related to technology.

## Purpose of the Policy

Camphill Wakefield have a robust process in place to ensure the online safety of students, staff, volunteers and trustees. We deliver an effective approach to online safety, which empowers us to protect and educate everyone in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' and tablets), 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:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. **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.
3. **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
4. **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 education providers on:

- Teaching online safety in education
- Preventing and tackling bullying and cyber-bullying: advice for education providers
- Relationships and sex education
- 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/tutors stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

## Roles and responsibilities

### The Trustee Board

The Board of Trustees has overall responsibility for monitoring this policy and holding the Chief Executive Officer to account for its implementation. The Board of Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online

safety logs as provided by the designated safeguarding lead (DSL) and the lead for online safety.

The trustee who oversees online safety is the responsible Trustee for Safeguarding.

All trustees will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of IT policy.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable students, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all students in all situations, and a more personalised or contextualised approach may often be more suitable.

**The Chief Executive Officer**

The Chief Executive Officer is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout Camphill Wakefield.

**The Designated Safeguarding Lead**

Details of Camphill Wakefield's DSL and deputies are set out in our safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety, in particular:

- Supporting the Chief Executive Officer in ensuring that staff understand this policy and that it is being implemented consistently throughout Camphill Wakefield.
- Working with the Chief Executive Officer, IT consultant and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Safeguarding Children and Adults policies.
- Ensuring that any online 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 Camphill Wakefield's behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety to the Chief Executive Officer and/local authorities.

This list is not intended to be exhaustive.

**The external IT organisation are responsible for:**

- Putting in place an appropriate level of security protection procedures, including regular password changes and filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at Camphill, including terrorist and extremist material.

- Ensuring that the Camphill's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring of Camphill's IT systems on a regular 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 – all entries are logged on CPOMS.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy.

Camphill Wakefield subcontracts IT to an external organisation. The CEO is responsible for ensuring that the following responsibilities are reflected in the service specification and monitored through subcontract management processes.

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 Camphill's IT systems and the internet and ensuring that students follow Camphill's terms on acceptable use.
- 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'.

This list is not intended to be exhaustive.

**Parent/carers and wards**

Expectations are that:

- Parents/carers and wards will notify a member of staff or the Chief Executive Officer of any concerns or queries regarding this policy.
- Ensure that they understood and agreed to the terms on acceptable use of the Camphill's IT systems and internet use.
- Make Camphill aware of any incidents or concerns they have regarding their child's use of the internet including social media

Parents/carers and wards 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 – Child net International

**Educating students about online safety**

Students will be taught about online safety through teaching methods that are fully considered and in line with their curriculum pathway, fully adapted to ensure this meets students' need.

- Understanding a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- 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.
- How to be able to install software to protect their devices.
- 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 which 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 internet will also be covered in other subjects where relevant.

**Educating Parents/Carers and Wards about online safety**

- Camphill will raise parents, carers and wards awareness of internet safety in letters or other communications home and in information via our website and via parent mail.
- Share suitable materials when there has been an issue with a student or group of students.
- Make this policy available to all.

If parents, carers or wards have any queries or concerns in relation to online safety, these should be raised in the first instance with the Chief Executive Officer and/or the DSL.

Advice will be provided by the lead for online safety.

**Child on child Abuse**

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 one person or group by another person or group, where the relationship involves an imbalance of power. See also the Behaviour 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.

- Camphill Wakefield will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Education Support Workers, Curriculum Manager or Head of College will discuss cyber-bullying with their team.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

Camphill Wakefield will also share information on cyber-bullying to parents/carers and wards 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, Camphill will follow the processes set out in the Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among students, Camphill Wakefield will use all reasonable endeavours to ensure the incident is contained.

The Lead 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. When necessary, the incident will be reported to the relevant social media platform to be taken down.

**Examining electronic devices**

Senior staff in education 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, pads 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 teaching, and/or
- Break any of Camphill's codes of conduct

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should delete that material, or retain it as evidence (of a criminal offence or a breach of the code of conduct) and/or report it to the police.

Any searching of students will be carried out in line with The DfE's latest guidance on screening, searching 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 students' electronic devices will be dealt with through the complaints procedure.

**Acceptable use of the internet at Camphill**

Use of Camphill Wakefield'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 students, staff, volunteers, trustees, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Policy Agreement in the Acceptable Use Policy.

**Students using mobile devices at Camphill.**

Students may bring mobile devices to college as it is recognised they may be needed by the student when travelling to and from Camphill, however on arrival all students must have these stored away during sessions and are only allowed to use during break and lunch times.

The devices remain the responsibility of the parent/carer or ward and Camphill Wakefield cannot be held responsible for loss or damage.

Any breach of the above by a student may trigger disciplinary action in line with the Behaviour Policy, which may result in the confiscation of their device during the hours they are on site.

**Staff using work devices off site.**

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).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- 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 – always install the latest updates.
- Staff members must not use the device in any way which would violate Camphill Wakefield's terms of acceptable use.
- 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 IT department.

**Misuse Management**

How Camphill Wakefield will respond to issues of misuse:

- Where a student misuses the IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use.
- Any incident that is deemed a safeguarding concern will also be recorded on CPOMS.
- The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The SLT member for IT will be notified of the issue:

- A decision will be made for the consequence.
- All blocked internet will be recorded on CPOMS.
- The Education support leads will contact home.

Where a staff member misuses Camphill Wakefield's IT 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 Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Camphill Wakefield 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 training, as part of their induction, 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).

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 and young adults are at risk of online abuse. Students 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 students can recognise dangers and risks in online activity 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 DSL 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

**Monitoring arrangements**

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

This policy will be reviewed every year by the DSL and Lead Trustee for Safeguarding. At every review, the policy will be shared with the Board of Trustees.

By an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

**Review**

This policy will be reviewed on an annual basis, in line with statutory requirements, by the Head of Performance for approval by the Trustee Safeguarding Committee.