EmpowerEd Online Safety Policy

Date of Publication: 12/03/2022

Review: 03/09/2024

Date of Next Review: 03/09/2025

Reviewed by: Paige Beaney

Approved by: Beth Mills

POLICY AIMS

This policy takes into account the DfE statutory guidance Keeping Children Safe in Education 2024.

EmpowerEd
Unlocking potential, building futures

The purpose of EmpowerEd's Online Safety policy is to:

- Safeguard and protect all members of EmpowerEd community online
- Identify approaches to educate and raise awareness of Online Safety throughout the community
- Ensure all staff have read and understood the Online Safety Policy
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Ensure that tutors providing in person tuition whilst using a laptop or other device, use the device in a safe and responsible way
- Recognises the specific risks that can be posed by mobile technology, including mobile phones.
- Identify clear procedures to use when responding to Online Safety concerns

EmpowerEd identifies that the issues classified within Online Safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material e.g. fake news, pornography, suicide, anti-semitism,radicalisation, extremism and racism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer abuse, including cyberbullying, and the use of mobile and smart technology, 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; 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.

POLICY SCOPE

EmpowerEd believes that Online Safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.

EmpowerEd identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

EmpowerEd believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the leadership team, tutors, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the company (collectively referred to as “staff” in this policy) as well as students, parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with company issued devices for use off-site, such as work laptops, tablets or mobile phones.

Links with other policies:

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Behaviour Policy
- Data Protection Policy
- Safeguarding Policy
- Staff Disciplinary Policy

MONITORING AND REVIEW

Technology in this area evolves and changes rapidly. EmpowerEd will review this policy at least every year.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will regularly monitor internet use and evaluate Online Safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of Online Safety, the Designated Safeguarding Lead, will be informed of Online Safety concerns, as appropriate.

Any issues identified via monitoring will be incorporated into our action planning.

ROLES AND RESPONSIBILITIES

The Designated Safeguarding Lead (DSL) has lead responsibility for Online Safety. The ultimate lead responsibility for safeguarding and child protection, including Online Safety remains with the DSL.

EmpowerEd recognises that all members of the community have important roles and responsibilities to play with regards to Online Safety.

Directors

The Centre Directors will:

- ensure that Online Safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- ensure there are appropriate and up-to-date policies regarding Online Safety; including a Behaviour Policy, which covers acceptable use of technology
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- ensure that Online Safety is embedded within a progressive curriculum, which enables all students to develop an age-appropriate understanding of Online Safety
- support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their Online Safety responsibilities
- ensure there are robust reporting channels for the community to access regarding Online Safety concerns, including internal, local and national support
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology •

audit and evaluate Online Safety practice to identify strengths and areas for improvement

Designated Safeguarding Lead (DSL)

The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- work alongside the DCPC to ensure Online Safety is recognised as part of the company 's safeguarding responsibilities and that a coordinated approach is implemented
- ensure all members of staff receive regular, up-to-date and appropriate Online Safety training
- access regular and appropriate training and support to ensure they understand the unique risks associated with Online Safety and have the relevant knowledge and up to date required to keep students safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online
- keep up-to-date with current research, legislation and trends regarding Online Safety and communicate this with the community, as appropriate
- ensure that Online Safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- maintain records of Online Safety concerns, as well as actions taken, as part of the company 's safeguarding recording mechanisms
- monitor Online Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- report Online Safety concerns, as appropriate, to the Leadership Team and Governing Body
- work with the Leadership Team to review and update Online Safety policies on a regular basis (at least annually) with stakeholder input
- meet annually with the directors with a lead responsibility for safeguarding and online safety

Staff Members

It is the responsibility of all members of staff to:

- contribute to the development of Online Safety policies
- read and adhere to the Online Safety policy and acceptable use policies
- take responsibility for the security of company systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- embed Online Safety education in curriculum delivery, wherever possible
- have an awareness of a range of Online Safety issues and how they may be experienced by the students in their care
- identify Online Safety concerns and take appropriate action by following the company 's safeguarding policies and procedures
- know when and how to escalate Online Safety issues, including signposting to appropriate support, internally and externally
- take personal responsibility for professional development in this area

It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate Online Safety policies and procedures
- implement appropriate security measures as directed by the DSL and Leadership Team, such as password policies and encryption, to ensure that the company's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure appropriate access and technical support is given to the DSL to the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required

Students

It is the responsibility of students (at a level appropriate to their age and ability) to:

- engage in age appropriate Online Safety education opportunities
- contribute to the development of Online Safety policies
- read and adhere to the acceptable use policies
- respect the feelings and rights of others both on and offline
- take responsibility for keeping themselves and others safe online
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing Online Safety issues

Parents/Carers

It is the responsibility of parents/carers to:

- read the acceptable use policies and encourage their children to adhere to them
- support the company 's Online Safety approaches by discussing Online Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the company , or other appropriate agencies, if they or their child encounter risk or concerns online
- contribute to the development of the Online Safety policies
- use company systems, such as learning platforms, and other network resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

EDUCATION AND ENGAGEMENT APPROACHES

Education and Engagement with students

EmpowerEd will establish and embed a progressive Online Safety curriculum to raise awareness and promote safe and responsible internet use amongst students by:

- ensuring education regarding safe and responsible use precedes internet access

- reinforcing Online Safety messages whenever technology or the internet is in use
- educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

EmpowerEd will support students to read and understand the acceptable use policies in a way which suits their age and ability by:

- displaying acceptable use posters in any room with internet access in an EmpowerEd premises (temporary or permanent)
- informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- rewarding positive use of technology
- providing Online Safety education and training as part of the transition programme across the key stages and when moving between establishments
- seeking student voice when writing and developing Online Safety policies and practices, including curriculum development and implementation
- using support, such as external visitors, where appropriate, to complement and support our internal Online Safety education approaches

Vulnerable students

EmpowerEd recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

EmpowerEd will ensure that differentiated and ability appropriate Online Safety education, access and support is provided to vulnerable students.

When implementing an appropriate Online Safety policy and curriculum, EmpowerEd will seek input from specialist staff as appropriate, including the SENCO.

Training and Engagement with Staff

We will:

- provide and discuss the Online Safety policy and procedures with all members of staff as part of induction
- provide up-to-date and appropriate Online Safety training for all staff on a regular basis, with at least annual updates - this will cover the potential risks posed to students (Content, Contact and Conduct) as well as our professional practice expectations
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape Online Safety policies and procedures
- make staff aware that our IT systems are monitored, and that activity can be traced to individual

users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices
- make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation
- highlight useful educational resources and tools which staff should use, according to the age and ability of the students
- ensure all members of staff are aware of the procedures to follow regarding Online Safety concerns affecting students, colleagues or other members of the community

Awareness and Engagement with Parents/Carers

EmpowerEd recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to Online Safety with parents/carers by:

- providing information and guidance on Online Safety in a variety of formats
- drawing their attention to the Online Safety Policy
- requesting that they read Online Safety information as part of joining our community, for example, within our home:provision agreement

REDUCING ONLINE RISKS

EmpowerEd recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the company is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the company's computers or devices.

All members of the community are made aware of the company's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the acceptable use policies and highlighted through a variety of education and training approaches.

SAFER USE OF TECHNOLOGY

Session Use

EmpowerEd uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites

- Learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

All company owned devices will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and applications fully before use in sessions or recommending for use at home.

We will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.

Supervision of students will be appropriate to their age and ability.

students will be appropriately supervised when using technology, according to their ability and understanding.

Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems.

All staff and students will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

Filtering and Monitoring

Levels of Internet access and supervision will vary according to the student's age and experience. Older students, as part of a supervised project, might need to access specific adult materials - for instance a course text or set novel might include references to sexuality - while tutors may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, the restrictions imposed by the company 's filtering system may be removed temporarily while the user accesses the material under close supervision.

The company will work with the local authority to ensure that systems to protect users are constantly under review.

Staff and students who discover that an unsuitable site is accessible must report this to the company's DSL.

The DSL will manage the configuration of the filtering system to ensure that it is appropriate, effective and reasonable.

The company will report any online material it believes to be illegal to the appropriate agencies.

Decision Making

EmpowerEd's DSL has ensured that the company has age and ability appropriate filtering and monitoring in place, to limit student exposure to online risks.

The DSL is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Leadership Team; all changes to the filtering policy are logged and recorded.

The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

Filtering

If students discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the DSL and the breach will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the Police or Child Exploitation and Online Protection command (CEOP).

Monitoring

We will appropriately monitor internet use on all company owned or provided internet enabled devices. This is achieved by keyword monitoring and tutoring management software.

If a concern is identified via monitoring approaches the DSL will be informed as appropriate.

All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

Full information can be found in our Data Protection Policy.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems

- Not using portable media without specific permission; portable media will be checked by an anti virus/malware scan before use
- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly checking files held on our network
- The appropriate use of user logins and passwords to access our network
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended

Managing the Safety of Our Network

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or student's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.

Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Behaviour Policy, Child Protection Policy, Data Protection Policy and Safeguarding Policy.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

Company email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external

personal email accounts may be blocked on site.

Staff Email

The use of personal email addresses by staff for any official setting business is not permitted.
All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.

Educational Use of Videoconferencing and/or Webcams

EmpowerEd recognises that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.

Video Conferencing contact details will not be posted publicly.

Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.

Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

Parents/carers consent will be obtained prior to students taking part in videoconferencing activities.

students will ask permission from a member of staff before making or answering a video conference call or message.

Videoconferencing will be supervised appropriately, according to the student's age and ability.

Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Only key administrators will be given access to videoconferencing administration areas or remote-control pages.

The unique login and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

When recording a video conference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must

be given and recorded material will be stored securely.

If third party materials are included, we will check that recording is permitted to avoid infringing the third party intellectual property rights.

We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the students.

To safeguard students' data:

- only student issued devices will be used for apps that record and store students' personal details, attainment or photographs
- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store students' personal details, attainment or images unless appropriately encrypted
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems
- parents/carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

SOCIAL MEDIA

Expectations

The expectations regarding safe and responsible use of social media applies to all members of the EmpowerEd community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of the EmpowerEd community are expected to engage in social media in a positive, safe and responsible manner.

All members of the EmpowerEd community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control student and staff access to social media whilst using company provided devices and systems on site.

Inappropriate or excessive use of social media during company hours or whilst using company devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of the EmpowerEd community on social media, should be reported to the DSL and will be managed in accordance with our Child Protection Policy for Managing Allegations against Staff, Anti-bullying, Behaviour and Safeguarding Policies.

EmpowerEd
Unlocking potential, building futures

Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the company.
Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the company

Members of staff are encouraged not to identify themselves as employees of EmpowerEd on their personal social networking accounts; this is to prevent information on these sites from being linked with the company, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with students and parents/carers

All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL.

If ongoing contact with students is required once they have left the company , members of staff will be expected to use existing alumni networks or use official settings provided communication tools.

Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the DSL.

Any communication from students and parents received on personal social media accounts will be reported to the DSL.

Students' Personal Use of Social Media

Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.

Any concerns regarding a student's use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications
- How to report concerns both within the setting and externally

Official Use of Social Media

EmpowerEd does have a couple of official social media accounts.

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The official use of social media as a communication tool has been formally risk assessed and approved by the DSL. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use settings provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and, where possible, run and linked to our website.

Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data Protection, Safeguarding and Child Protection.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Written parental consent will be obtained, as required.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving students will be moderated

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
If members of staff are participating in online social media activity as part of their capacity as an employee of the company , they will:

- sign our social media acceptable use policy
- always be professional and aware they are an ambassador for the company
- disclose their official role and position but make it clear that they do not necessarily speak on behalf of the company
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared
- always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws
- ensure that they have appropriate consent before sharing images on the official social media channel
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- not engage with any direct or private messaging with current students, parents/carers • inform the DSL and /or IT Support Manager of any concerns, such as criticism, inappropriate content or contact from students

USE OF PERSONAL DEVICES AND MOBILE PHONES

EmpowerEd recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within the company..

Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti

bullying, Behaviour and Child Protection and Safeguarding.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

All members of the EmpowerEd community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

All members of the EmpowerEd community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

All members of the EmpowerEd community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour, Safeguarding or Child protection Policies.

Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Data Protection, Safeguarding and Child Protection Policy for Managing Allegations against Staff.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time • Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times
- Not use personal devices during teaching periods, unless permission has been given by the DSL such as in emergency circumstances
- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations

Members of staff are not permitted to use their own personal phones or devices for contacting students or parents/carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL.

Staff will not use personal devices:

- to take photos or videos of students unless permission has been given by the DSL, and will only use work-provided equipment for this purpose
- directly with students and will only use work-provided equipment during lessons/educational activities

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or has committed a criminal offence, the police will be contacted.

students' Use of Personal Devices and Mobile Phones

students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

EmpowerEd expects students' personal devices and mobile phones to be kept in a secure place and kept out of sight during lessons.
Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a student breaches the policy, sanctions and interventions will be applied.

Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or anti-bullying policy or could contain youth produced sexual imagery (sexting). The following would apply:

- Searches of mobile phone or personal devices will only be carried out in accordance with our Behaviour, Child Protection and Safeguarding Policies
- Student's mobile phones or devices may be searched by a member of the Leadership Team, with the consent of the student or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our Behaviour, Child Protection and Safeguarding Policies
- Mobile phones and devices that have been confiscated will be released to parents/carers
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: Anti bullying, Behaviour, Child Protection and Safeguarding.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL.

Officially Provided Mobile Phones and Devices

Members of staff will be issued with a work phone number and email address, where contact with students or parents/carers is required. In addition, occasionally company provided mobile phones/devices will be issued to staff where appropriate.

Company mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

company mobile phones and devices will always be used in accordance with the relevant policies.

RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. students, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents/carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.

Where there is suspicion that illegal activity has taken place, the DSL will contact the Education Safeguarding Team or the local Police force using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local organisations are involved or the public may be at risk), the DSL will speak with Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Concerns about students' Welfare

The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns. The DSL will record these issues in line with our Safeguarding and Child Protection policies.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the local Safeguarding Children Board thresholds and procedures.

The DSL and/or DCPC will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

Any complaint about staff misuse will be referred to the DSL.

Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

Appropriate action will be taken in accordance with our Child Protection Policy for Managing Allegations against Staff, Behaviour, Safeguarding policies.

EmpowerEd
Unlocking potential, building futures

PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

Online Sexual Violence and Sexual Harassment Between Children

Our company has accessed and understood 'Sexual violence and sexual harassment between children in company s and colleges' (2018) guidance and part 5 of 'Keeping Children Safe in Education' 2023. The company recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Behaviour, Child Protection and Anti-bullying Policies.

The company recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

The company also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

The company will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL and act in accordance with our Behaviour, Child Protection and Anti bullying Policies
- If content is contained on students' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Implement appropriate sanctions in accordance with our behaviour policy
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- If appropriate, make a referral to partner agencies, such as Children's Social Services and/or the Police
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- If a criminal offence has been committed, the DSL will discuss this with Kent Police first to ensure that investigations are not compromised

- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

Youth Produced Sexual Imagery

The company recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

We will follow the advice as set out in the non-statutory UK Council for Child Internet Safety (UKCCIS) guidance: 'Sexting in companies and colleges: responding to incidents and safeguarding young people'.

The company will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using company provided or personal equipment.

We will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented
- send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our safeguarding and child protection policies and the relevant Kent Safeguarding Children Board's procedures
- ensure the DSL responds in line with the 'Sexting in company s and colleges: responding to incidents and safeguarding young people' guidance
- store the device securely
- if an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image
- carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies
- inform parents/carers, if appropriate, about the incident and how it is being managed • make a referral to Children's Social Services and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in company s and colleges: responding to incidents and safeguarding young people' guidance
- provide the necessary safeguards and support for students, such as offering counselling or pastoral support
- implement appropriate sanctions in accordance with our Behaviour Policy but taking care not to further traumatised victims where possible
- consider the deletion of images in accordance with the UKCCIS: 'Sexting in company s and colleges:

responding to incidents and safeguarding young people' guidance

• delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation • review the handling of any incidents to ensure that best practice was implemented; the Leadership Team will also review and update any management procedures, where necessary

Online Sexual Abuse and Exploitation (Including Criminal Exploitation)

The company will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

The company recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- act in accordance with our child protection policies and the relevant Kent Safeguarding Children Board's procedures
- if appropriate, store any devices involved securely
- make a referral to Children's Social Services (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk
- carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies)
- inform parents/carers about the incident and how it is being managed
- provide the necessary safeguards and support for students, such as, offering counselling or pastoral support
- review the handling of any incidents to ensure that best practice is implemented; Leadership Team will review and update any management procedures, where necessary

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using company provided or personal equipment.

Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.

If students at other settings are believed to have been targeted, the DSL will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

The company will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

If it is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Police and/or the Education Safeguarding Team.

If made aware of IIOC, we will:

- act in accordance with our child protection policy and the relevant local Safeguarding Child Boards procedures
- store any devices involved securely
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO

If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:

- ensure that the DSL is informed
- ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- ensure that any copies that exist of the image, for example in emails, are deleted
- report concerns, as appropriate to parents/carers

If made aware that indecent images of children have been found on the company provided devices, we will:

- ensure that the DSL is informed
- ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- ensure that any copies that exist of the image, for example in emails, are deleted
- inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Services (as appropriate)
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- report concerns, as appropriate to parents/carers

If made aware that a member of staff is in possession of indecent images of children on company

provided devices, we will:

- ensure that the DSL are informed in line with our Child Protection Policy for Managing Allegations Against Staff
- inform the LADO and other relevant organisations in accordance with our Child Protection Policy for Managing Allegations Against Staff
- quarantine any devices until police advice has been sought

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at the company .

Full details of how we will respond to cyberbullying are set out in our anti-bullying and safeguarding policies.

Online Hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at the company and will be responded to in line with existing policies, including Anti-bullying and Behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or local Police.

Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding Policies.

If we are concerned that members of staff may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the Child Protection Policy for Managing Allegations against Staff and Safeguarding Policy.

ONLINE SAFETY LINKS AND CONTACTS

CEOP (Child Exploitation and Online Protection Centre)	www.ceop.police.uk
Child Exploitation and Online Protection (CEOP)	www.ceop.police.uk www.thinkuknow.co.uk

EmpowerEd
Unlocking potential, building futures

Childnet	www.childnet.com
NSPCC	www.nspcc.org.uk/onlinesafety
Childline	www.childline.org.uk
UK Safer Internet Centre	www.saferinternet.org.uk
Internet Watch Foundation	www.iwf.org.uk
Internet Matters	www.internetmatters.org
Net Aware	www.net-aware.org.uk

The Designated Safeguarding Lead (DSL) contact details:
Email: chris@empowered-education.co.uk
Telephone: 07423271640