Online Safety Policy – Whole School

Embleton View

For the purpose of this document, '*students*' refers to all children at Embleton View. However, we refer to primary age children as '*pupils*', and secondary age children as '*students*'.

The purpose of this policy is to safeguard students and staff at Embleton View. It details the actions and behaviour required from students and members of staff to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements, we have a whole school approach to Online Safety.

Our key message to keep students and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our Online Safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding & Child Protection Policy and other related documents.

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding & Child Protection Policy and our Prevent Policy. The staff and student Acceptable Use Policies (AUPs) are central to the Online Safety policy and should be consulted alongside this policy.

We consider how we can promote online safety whilst developing our curriculum, through our staff training, and through parental engagement. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important regarding the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding and Child Protection Policy, Preventing Extremism and Tackling Radicalisation Policy.

Roles and Responsibilities

The DSL has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice in compliance with Keeping Children Safe in Education (KCSIE 2024, DfE), ensuring that:

- Students know how to use the Internet responsibly and that parents/carers and Learning & Development Coordinators (LDCs) have the right measures in place to keep students safe from exploitation or radicalisation.
- Students are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- Students use Information and Communications Technology (ICT) safely and securely and are aware of both external and child to child risks when using ICT, including cyberbullying and other forms of abuse.
- Children, staff and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or encounter the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

The Proprietors responsibilities

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Proprietors will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the Proprietors have ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

All Staff

It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate Internet access or use, both inside and outside of Embleton View, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current online safety issues, and this Online Safety Policy. Cyber-bullying incidents will be reported in accordance with Embleton View's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to their line manager which will be placed on staff files. LDCs will ensure they are confident in promoting and delivering online safety as required, identifying risks and reporting concerns as they arise.

Parents/Carers

Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. Embleton View will support parents/carers by sharing information and links through newsletters, email and the school's website. Parents/carers will need to provide Embleton View with written consent to allow their child to access IT resources at school.

All Students

Students are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Breadth of Online Safety Issues

We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, material against any faith or religion, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: child to child 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; 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; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

These issues are to be managed through the school's filtered Internet (CISCO Umbrella), by promoting safe and responsible use, and ensuring both staff and students can report any concerns to the appropriate people.

Staff/Volunteers Use of IT Systems

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the Staff Code of Conduct before using any school ICT resource. In addition:

- All staff will receive appropriate Online Safety training, which is updated regularly.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other devices.
- In sessions where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the students visit.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Any request to do so should be made to the Director of Operational Development (DOD).
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved software and email systems which have appropriate security in place.
- Files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Staff should only communicate electronically with students through the school approved platforms.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of sessions, activities, or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the DSL or DDSL
2. The DO should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the Child Exploitation and Online Protection Command (CEOP) and the police will be informed.
5. No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and the police will be contacted.

Teaching about Online Safety

Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching students about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Access levels to ICT reflect the curriculum requirements and age of students. Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity. This teaching is built into existing sessions alongside our wider whole-school approach. Students will explicitly be taught the following topics through their sessions:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use.
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications.
- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- Online behaviour.
- How to identify online risks.
- How and when to seek support; and
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that child on child abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the Internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

Staff should be vigilant in sessions where students use the Internet. If staff allow the use of school mobile devices in their sessions, they must ensure that they are used in line with school policy. The use of personal phones is prohibited.

Harmful online challenges and online hoaxes

There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach students to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within online safety sessions, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents/carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents/carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Students Use of IT Systems

All students must agree to the IT Acceptable Use Policy before accessing the school systems. Students at Embleton View will be given supervised access to our computing resources and will be provided with access to filtered Internet and other services operating at the school. Problems with ICT equipment should be reported either to the LDC or the DO. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of students and young people. The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law. Embleton View will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff

Staff will be provided with sufficient online safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the Internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the Internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

Communicating and Educating parents/carers in online safety
We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website). Parents/carers will also be provided with a copy of the age-relevant Student IT Acceptable Use Policy, and parents/carers will be asked to sign it, as well as the students. Embleton View recognises the crucial role that parents/carers play in the protection of their children with regards to online safety. Parents/carers are always welcome to discuss their concerns on online safety with the school, who can direct them to the support of our DSL if required. Parents/carers will be encouraged to support the school in promoting good online safety practice.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) 2020. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our online safety sessions and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will be responsible for ensuring there is an appropriate level of security procedures in place, to safeguard systems, staff and learners and will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Radicalisation and the Use of Social Media to Encourage Extremism
The Internet and the use of social media has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and promote extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people.
- Promoting extreme beliefs.
- Accessing likeminded people where they are not able to do this off-line, creating an online community.
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Embleton View has a number of measures in place to help prevent the use of social media for this purpose:

- Website filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by students.
- Students, parents/carers and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation
Embleton View has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding online safety should be made to the DSL, who will review the issue and take the appropriate action. For students, they are taught to raise any concerns to their LDC who will then pass this on to the DSL or Headteacher. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our DSL provides advice and support to other members of staff on protecting students from the risk of online radicalisation. Embleton View ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of students and know to report any concerns to the DSL.

Assessing Risks

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

- Personal mobile phones are not permitted in school.
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Proprietors will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems apart from filtered Wi-Fi access, if necessary.
- Embleton View takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable "over-blocking".
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the system's filtering with behaviour management and additional staff/student training. Students must give any personal mobile devices to the responsible staff member when arriving at school and may collect them on their way back at the end of the day.

Mobile Electronic Devices

Personal mobile phones are not permitted to be used by any students during the school day. Students must give any personal mobile devices to the responsible staff member when arriving at school and may collect them on their way back at the end of the day or during agreed breaktimes. Mobile phones are kept on site at the risk of the individual student. Embleton View is not responsible for any devices lost or damaged whilst on school grounds.

Recordings made using mobile electronic devices

Using the camera on a personal phone or similar device, either to photograph/film/record any member of the school community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. Any recording can only be made on a school mobile phone under the supervision of a member of staff and must be for the purposes of learning evidence only. All recorded media made on a school mobile phone is to be uploaded to the appropriate folder on the school drive immediately and removed from the phone. The discovery of any uploads to personal social media platforms will result in serious sanctions being applied. Embleton View use Twitter / X to share news with parents/carers. Recorded media can be uploaded to Twitter to show learning opportunities but must only include students whose parents/carers have provided written consent.

Cyber-Bullying

Cyber-bullying the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset, intimidate or harass someone else. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort. This also includes Sexting.
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks. 'Upskirting' involves taking unauthorised photos of under another person's clothing.
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to students or young people when they are in a web-based chat room.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, text messaging etc.) as they conduct real-time conversations online.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** includes the use of defamatory blogs, personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Students should remember the following

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

Online Sexual Harassment

Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will be dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a) The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferInternet.org.uk. Providing expert advice and support for school staff regarding online safety issues and when an allegation is received.

b) If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will assess whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT-Based Sexual Abuse (Including Sexting)

The impact on a child of ICT-based sexual abuse is like that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile phone.
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images.
- An adult or older child may be viewing and downloading child sexual abuse images.

Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice who in turn will speak to the DSL and Headteacher.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which can lead to a criminal prosecution.

Consequences

Consequences will depend on the severity of the offence as assessed by the Senior Management Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the school.
- Temporary or permanent ban on the use of the internet in the school.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

Chat Room Grooming and Offline Abuse

Staff need to be continually alert to any suspicious activity involving computers and the internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur for the abuser to harm the child.

Social Media, including Facebook, Twitter and Instagram:

Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Headteacher for reasons of work
- Staff are advised not to befriend or follow parents/carers of students and to keep their personal profile as private as possible
- Staff and students are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and students, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

Staff and students are aware that their online behaviour should always be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Code of Conduct. Embleton view recognises that social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Artificial intelligence (AI)

Our school recognises that generative artificial intelligence (AI) tools, such as Google Bard and ChatGPT, have many uses. These include enhancing teaching and learning and helping to protect and safeguard students. However, it is crucial that we are aware of the risks carried by AI; for example, facilitating abuse in the form of bullying or grooming, and exposing students to harmful content. This could be in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. It is important that all staff are aware of the risks posed by AI tools, and that risk assessments are carried out for all new AI tools used by our school. Any use of AI to access harmful content or bully students will be treated in line with this policy and our anti-bullying policy.

Taking and Storing Images of Students Including on school mobile phones

Embleton View provides an environment in which students, parents/carers and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents/carers, volunteers and visitors are informed that they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students. This prevents staff from being distracted from their work with students and ensures the safeguarding of students from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.
- Any Looked After Child (LAC) will not have their photos used on school social media or the website without written authorisation from their primary carer and/or social worker.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Use of Mobile Devices Policy which includes:

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Embleton View, taking into consideration staff, students on placement, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding & Child Protection Policies.

Remote Learning (Please see our Offsite Learning and Activities Policy for more details)

Where there are periods in which the school is forced to close yet continue to provide education (such as during the COVID-19 Pandemic) it is important that Embleton View supports staff, students and parents/carers to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on students' mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection and Safeguarding Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and students respective Behaviour/Codes of Conduct. Additionally, Embleton View will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Embleton View will put additional measures in place to support parents/carers and students who are learning from home. This will include specific guidance on which programmes the school is expecting students to use and how to access these alongside how students and parents/carers can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual sessions (including video conferencing). Details of this can be found in our schools Offsite Learning and Activities Policy.

Additionally, the Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day-to-day responsibility being delegated to the DSL. The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, if it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

Legal Status;

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Students Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: September 2024) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Students* (WT) (HM Government: September 2018) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (2023) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2023) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in Schools (2020)
- Harmful Online challenges and online hoaxes (2021)

Applies to:

- The whole school and all other activities provided by the school, inclusive of those outside of the normal school hours.
- All staff (teaching, support and admin staff), students, the proprietors, agency staff and volunteers working in the school.
- Visitors and contractors accessing the site.

Availability

- This policy is made available to parents/carers, staff and students as a hardcopy upon request from the school office.

Monitoring and Review:

This policy will be subject to continuous monitoring, refinement and audit by the Headteacher. The Headteacher and/or the Proprietors and/or a suitably appointed delegate will undertake a formal review of the policy, by no later than two years from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Related Documents:

- Child Protection and Safeguarding Policy
- PREVENT Policy
- Data Protection Policy
- Data Retention Policy
- Use of Mobile Devices Policy
- Computing Policy
- Offsite Learning & Activities Policy

Embleton View is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential

		
Graeme Turner (Proprietor)	Anna Turner (Proprietor)	Craig Bell (Proprietor)
Date Published: 02/08/17	Date Published: 02/08/17	Date Published: 02/08/17
Reviewed:	Reviewed:	Reviewed: 12/8/2018 Reviewed: 04/08/2019 Reviewed: 27/07/2020 Reviewed: 05/01/2021 Reviewed: 05/01/2021 Reviewed: 05/01/2021 Reviewed: 28/07/2021 Reviewed:29/06/2022 Reviewed: 06/07/23 Reviewed: 02/09/2023 Reviewed: 27/03/2024 Reviewed: 29/08/2024