CASTLE VIEW Group

Online Safety Policy

Responsible officer	Martin Wright
Approved by	Susan Kirby
Approved date	19.4.24
Next review date	19.4.25

Version	Amendment	Pages	Date	Who
2	Update of content	all	19.4.24	MW

I.INTRODUCTION

CastleView Group (CVG) has an online safety policy to protect learners and staff. The policy recognises that online safety encompasses not only the Internet but any type of electronic communication.

It is important for all learners to understand the Internet is an unmanaged, open communications channel. Anyone can send messages, discuss ideas and publish material with no restriction. These features of the Internet make it an invaluable resource used by millions of people every day - however not all information is correct, accurate or valid.

Learners should be aware that publishing personal information could compromise your security and that of others.

Applies to:

All employees and learners on site and remote locations

Context:

Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings staff and learners into contact with a wide variety of influences some of which may be unsuitable.

II. POLICY STATEMENT

CVG will continually make it clear to all learners, staff and visitors that the use of CVG equipment for inappropriate reasons is unacceptable. CVG will take reasonable actions and measures to protect all its users, including (although not limited to) disciplinary action. Learners must report to a tutor or a safeguarding officer if a member of staff attempts to communicate with them via social media.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

These technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning environment. Current and emerging technologies in education and more importantly, in many cases used outside the learning environment by learners, include (but are not limited to):

- Internet websites
- Virtual Learning Environments
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.
- Intranet and collaboration applications such as MS Teams
- social media communications, by learners inside and outside of the learning environment.

III. CONTENT

Responsibilities
The reporting responsibilities for online safety follow the same lines of responsibility as for Safeguarding.

All Staff

- Responsible for ensuring the online safety of learners
- MUST report any concerns or disclosures immediately to a DSL
- NEVER offer assurance of confidentiality everything discussed MUST be reported
- MUST keep to the terms and conditions of the IT Acceptable Use Policy at all times
- MUST attend staff training on online safety and display a model example to learners at all times.
- MUST actively promote through embedded good e-safety practice.
- MUST communicate with learners and stakeholders professionally and in line with our expectations

Learner:

- Must receive appropriate online safety guidance as part of their programme of study
- Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another learner.
- Learners must act safely and responsibly at all times when using the internet and/or mobile technologies.

Designated Safeguarding Leads (DSL)

- MUST follow the safeguarding Reporting Procedure at all times
- With management approval refer to appropriate additional support from external agencies.
- Calling e-safety meetings when required
- Ensuring delivery of staff development and training
- Recording incidents
- Reporting any developments and incidents to the Senior Management Team
- Liaising with the local authority and external agencies to promote online safety
  IT services
- Ensure our IT infrastructure is secure and meets best practice recommendations
- IT security incidents are recorded, investigated and resolved within reasonable a reasonable timescale
- MUST report any online safety concerns or disclosures immediately to a DSL

Online Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Learners must report to any member of staff if they view any extremist or radical views expressed online. Staff should report any concerns immediately to a member of the safeguarding team.

There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer.

The Internet and the use of social media in particular has become a major factor in the radicalisation of young people. Radicalised learners can also act as a focal point for further radicalisation through personal contact with fellow learners and through their social media activity. Where radicalisation happens away from the classroom, the learner concerned may well share issues with other learners. This guidance therefore addresses the need for institutions in receipt of public funding to self-assess and identify the level of risk, ensure all staff have access to training, and that there is welfare support for learners. It is also key that we have effective IT policies in place which ensure that these signs can be recognised and responded to appropriately (Prevent Duty Guidance: for further education institutions in England and Wales 2015)

Child Sexual Exploitation

Child Sexual Exploitation (CSE) may involve utilising the Internet and social media to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline.

Means of accessing the Internet may also be provided to children as a “gift” by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE can take place entirely online such as children and young people being coerced into performing sexual acts via webcam/Social Media.

Cyber Bullying
Cyber bullying is a form of bullying. As it takes place online, it is not confined to organisation buildings or organisation hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

Cyber bullying includes bullying via:

- Text message and messaging apps e.g. sending unwelcome texts or messages that are threatening or cause discomfort.
- Picture/video-clips e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites.
- Phone call e.g. silent calls or abusive messages. The bully often disguises their number.
- Email e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them.
- Chat room e.g. sending upsetting responses to people when they are in a web-based chat room.
- Instant Messaging (IM) e.g. sending unpleasant messages in real-time conversations on the internet.
- Websites e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

Where conduct is found to be unacceptable, we will deal with the matter internally and refer to relevant policies, for example, the Disciplinary Policy. Where conduct is considered illegal, we will report the matter to the police.

Youth Produced Sexual Imagery and Sharing of Inappropriate Imagery
Where we have a “Lawful basis for processing” the use of images, or photographs, is popular in teaching and learning and should be encouraged. This will include images downloaded from the internet and images belonging to staff or learners.

Images & Videos of learners must be stored within approved systems and must never been stored or sent to personal devices or accounts.

Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe – e.g. there are particular risks where personal images are posted onto social networking sites.

No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner of that image. Photographs of activities on our premises should be considered carefully and have the consent of the leadership team before being published. Approved photographs should not include names of individuals.

Youth Produced Sexual Imagery (YPSI – formerly known as ‘Sexting’) can be defined as ‘an increasingly common activity among children and young people, where they share inappropriate or explicit images online’. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.

Although viewed by many young people as a ‘normal’ or ‘mundane’ activity and part of ‘flirting’, YPSI can be seen as harmless; but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend;
- share an explicit image or video of a child, even if it’s shared between children of the same age.
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

Any learner found attempting to access inappropriate or harmful material will be subject to disciplinary procedures.

This list is updated regularly:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age or sex
- Drugs/Substance abuse: Displays or promotes the illegal use of drugs or substances
- Extremism: Promotes terrorism and terrorist ideologies, violence or intolerance
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: Includes illegal provision of copyrighted material
- Self-Harm: Promotes or displays deliberate self-harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill
- N.B. This list is not exhaustive

Raising Awareness

Online safety awareness is delivered to all learners in a range of ways including through tutorial/feedback/progress sessions which focus on Online Reputation, Exploitation, Online Gaming and Sleep Awareness.

Issues associated with online safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Targeted events such as ‘Safer Internet Week’ and ‘Stay Safe Week’ are promoted with a range of activities, information and external professionals providing advice and guidance to both learners and staff.

Learners are expected to adopt an attitude of ‘collective responsibility’ towards online safety by encouraging others to stay safe and report any concerns to a member of Castle view staff.

Regular training is provided for all staff in regard to online safety, safeguarding, sexual and criminal exploitation and radicalisation.

Behaviour

Use of any CVG IT equipment and systems is conditional to our Policies including the IT User Policy & the Anti-Bullying Harassment Policy and Procedure.

Communications by staff and learners should be courteous and respectful at all times whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Anti-Bullying and Harassment Policy (staff and learners).

Staff should beware of our responsibility of the Prevent Duty and Safeguarding of young people and adults at risk.

The following guidance must be adhered by all staff communicating online:

- Staff must not post any personal views, beliefs or opinions
- Staff must challenge any personal views, beliefs or opinions posted by learners
- Staff must post with counter arguments to any personal view, beliefs or opinions posted by learners which undermine British Values
- Any post considered to isolate or put a young person or vulnerable adult at risk should be referred to a Safeguarding Officer for further investigation
- Any post considered to promote extreme views should be referred to a DSL for further investigation

Data Protection

We will comply with the Data Protection Act 2018 and GDPR by ensuring that personal data is: - Collected and processed lawfully, fairly and transparently for only specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Further processing for archiving purposes in the public interest, research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. - Adequate, updated and relevant and not excessive for the purposes it was collected. - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Including not being transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data. - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Confidentiality

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018. 9.2 These are not only restrictions on disclosure of information about CVG, they are bound by a common law duty of confidentiality. This duty prevents CVG from releasing information about staff and learners, without their consent. This duty applies to manual records as well as information held on computers.

Information which must be treated as confidential includes the names and addresses of employees and learners and any other information about them which is not publicly known aka "personal data". Accordingly, to ensure that we do not breach our duty, no information, even if it only exists in printed form, should be disclosed unless all the relevant procedures have been followed.

Since 1 January 2005 people have the right, under the Freedom of Information Act 2000, to request any information held by a public authority which it has not already made available through its publication scheme.

Internet Watch Foundation https://www.iwf.org.uk/

Get Safe Online https://www.getsafeonline.org/