E-safety / Social Media Policy

Social media is a term for any websites or applications which enable users to create and share content and take part in social networking. Some examples of social media are sites such as Facebook, Instagram, Twitter, LinkedIn, Youtube, TikTok and Pinterest. Social media also covers blogs and messaging apps such as Slack, Whatsapp.

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide team members and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- Ensure that no team member, learner, client or MBKB as a company are defamed through the use of social media and the internet.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in MBKB's activities.

MBKB recognise that:

The online world provides many opportunities; however it can also present risks and challenges. We recognise our duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online. We have a responsibility to help keep children and young people and adults safe online, whether or not they are using our network and devices. All people involved with MBKB, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will keep children, young people and adults safe by:

-Appointing an online safety coordinator - Katie Biggs (Designated safeguarding lead)
- Providing clear and specific directions to team members and volunteers on how to behave online through our code of conduct. This is also discussed at induction.
- Supporting and encouraging individuals who work with MBKB to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- Reviewing and updating the security of our information systems regularly, ensuring that usernames, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and young people who are involved in our organisation is held securely and shared only as appropriate

- Providing supervision, support and training for team members and volunteers about online safety
- Informing team members that they must not share any confidential information about learners, employers or any third party or partner of MBKB. This also includes any confidential information relating to MBKB as a company. Doing so would breach the Data Protection Act 1998.
- Team members should only use their MBKB company email and phone when communicating with employers and learners as part of their work role.
- We ask that all staff use MBKB electronic equipment for the purpose for which they are intended, as outlined in their staff induction.

Social Media Code Of Conduct

- Team members should avoid communicating with employers or 'in learning learners' on their personal social media accounts, with the exception of the below:-

- We allow for MBKB team members to communicate with learners and employers through Linked In, as this is a professional networking site, Facebook Pages set up by MBKB and Slack, used for networking.

- All MBKB team members are provided with this policy as part of their induction and its contents are discussed. All team members are required to agree to a social media code of conduct, outlining how they agree to use the above social media platforms only for work related purposes. This social media code of conduct states that the team member can only communicate with 'in learning' learners and employers through LinkedIn, Facebook Pages set up by MBKB and Slack for work related reasons and must always maintain a professional image when using them. They are only to communicate about training related topics and are not to disclose or request personal information. MBKB team members are in a position of trust and should not abuse their position at any time by making inappropriate contact via social media. If at any time a team member is concerned, they must report their concerns to the Safeguarding Team within 48 hours.

- Learners are also to report any concerns regarding social media contact – they are informed of how to do this within their enrolment paperwork, on the Commitment. Statement. MBKB take all reports of concerns regarding this very seriously and will treat it as a safeguarding concern. We will carry out a thorough investigation. Please see the safeguarding policy for the procedure for investigations of this nature.

- MBKB understand that there may be occasions where staff have already established relationships with employers or learners and, in this case, accept that social media may be used in these circumstances. An example of this would be if a staff member was previously a colleague of an employer MBKB may work with or if a staff member is a family friend of an MBKB learner or employer. If this is the case, we still urge learners, employers and team members to report any concerns using the same process as above.

- When posting on social media we ask that staff avoid material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying.

- Teaching e-safety as part of safeguarding within sessions and reviews. We also ask learners to complete 4 Education and Training Foundation modules, one of which is 'Staying safe online'.

- Provide a bank of E-safety resources which can be issued to learners and discussed with their tutor. We have provided a signposting link to CEOP Internet Safety and Online Protection site on our website so that our learners can easily access clear information and advice if they are concerned about e-safety

Cyberbullying

MBKB will not tolerate any harassment or bullying and are committed to ensuring all of its staff, employers and learners are treated with respect. Cyberbullying includes but is not limited to sending anonymous messages, posting negative comments or photos online, sharing photos without consent, harassment online and sending abusive or threatening messages electronically through the use of emails, apps, phone calls or websites.

We ask our staff to recognise the law regarding cyberbullying outlined in the Malicious Communications Act 1988 and understand it is against the law to use social media to harass others or cause intentional distress or anxiety to others. We ask that any staff experiencing cyberbullying within MBKB or any staff that suspect learners are experiencing cyberbullying to follow our safeguarding policy and record concerns within 24 hours then report to the DSL.

Disciplinary Action

As with all MBKB policies and protocols, breach of these terms and of the social media code of conduct may result in disciplinary action. For this purpose, note that both virtual and online communications are considered equal to face-to-face interactions.

Inappropriate use of social media, that related to MBKB, its learners, clients or team members, whether on official MBKB platforms or via your own social media networks is also covered by this policy and may result in disciplinary action.

Signed  Mark Bremner - CEO