IBCM ONLINE SAFETY POLICY

1. Purpose and context

1.1. The purpose of this policy is to outline the approach of International Business College Manchester (IBCM) in respect of ensuring that in the use of Information Technology and online activity, all users are safe and protected from harm.

1.2. IBCM recognises the benefits and opportunities which new technologies offer to staff, customers, learners and stakeholders. We provide internet access to all customers, learners and staff accessing services within our premises and the use of technologies in order to enhance skills, promote achievement and enable lifelong learning is encouraged. However, the accessibility and global nature of the internet, social media and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

1.3. IBCM identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

1.3.1. Content: being exposed to illegal, inappropriate or harmful content. For example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

1.3.2. Contact: being subjected to harmful online interaction with other users. For example child on child abuse, 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.

1.3.3. 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.

1.3.4. Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.4. It is essential that children and adults at risk are safeguarded from potentially harmful and inappropriate material or behaviours online. IBCM will adopt a whole organisational approach to online safety which will empower, protect, and educate our customers, learners and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

1.5. It is the intention of this policy to promote high standards of personal and professional practice across the institution in relation to the use of technology and outlines the procedures to follow when any concerns arise.

1.6. This policy should be read in conjunction with the IT User agreement and the Prevent and Safeguarding policies (as well as other policies identified below).

2. Scope

2.1. This policy applies to all members of IBCM (including staff, customers, learners, volunteers, and Stakeholders) who have access to and are users of IBCM ICT systems, both in and out of the organisation.

2.2. We have a responsibility to help keep children, young people and adults safe online, whether or not they are using IBCM network and devices

3. Definitions

3.1. Cyberbullying

3.1.1. Cyberbullying or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else. It is often linked to discrimination and like other forms of bullying, affects self-esteem and can affect mental health and wellbeing. Addressing all forms of bullying and discrimination is vital to support the health and wellbeing of the IBCM community.

3.2. Unsafe Communities

3.2.1. An online community can act as an information system where members can post, comment on discussions, give advice or collaborate. Commonly, people communicate through social networking sites, chat rooms, forums, e-mail lists and discussion boards. People may also join online communities through video games, blogs and virtual worlds.

3.2.2. Users also need to be aware of the dangers of unsafe communities such as extremist and criminal groups

3.3. Use of Digital and Video Images

3.3.1. The development of digital imaging technologies has created significant benefits to work and learning, allowing the use of images that have been recorded or downloaded from the internet. Customers, learners, staff and stakeholders need to be aware of the risks associated with publishing inappropriate content on the internet. Such images may provide avenues for cyber bullying, child on child abuse, child sexual exploitation, sexual violence & sexual harassment or grooming to take place.

3.3.2. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. IBCM will inform and educate users about these risks to reduce the likelihood of the potential for harm.

3.4. Sexting

3.4.1. Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, and laptops - any device that allows you to share media and messages. This includes videos or live streams via social media, gaming platforms, chat apps or forums. It could also include sharing between devices via services like Apple's AirDrop which works offline.

3.4.2. Making, possessing and distributing any imagery of someone under 18 which is indecent is illegal. The Sexual Offences Act 2003 defines a child for the purpose of indecent images as anyone under the age of 18. The non-consensual sharing of private sexual images or videos with the intent to cause distress is also illegal. However young people should not be unnecessarily criminalised.

3.4.3. IBCM recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; **all** concerns will be reported to and dealt with by the DSL (or deputy) irrespective of whether an under 18 year old is involved.

3.4.4. In many cases, educations settings may respond to incidents without involving the police, for example where an incident can be defined as experimental. However where there are abusive or aggravating factors, incident should always be referred to the police through the local safeguarding partnerships.

3.5. Online predators/Grooming

3.5.1. When users go online, they have direct and immediate access to friends, family, and complete strangers, which can put unsuspecting young people and adults at great risk. Young people who meet and communicate with strangers online are easy prey for Internet predators. Predators have easy and anonymous access and can conceal their identity and roam without limit.

3.5.2. Posts made by young people may expose personal information and put them at risk. For example, they may talk about their home life, feelings, or thoughts they've been having. This can include feelings of loneliness due to being in a strange country with a new culture. Perpetrators may use this information to groom, abuse or exploit.

3.5.3. Perpetrators of abuse may create fake profiles to try to contact children and young people through the platform you're using, for example an adult posing as a child. They may also create anonymous accounts and engage in cyberbullying, grooming or trolling. People known to a child can also perpetrate abuse

3.6. Cybercrime

Common forms of cybercrime include:

a) phishing: using fake email messages to get personal information from internet users;
b) misusing personal information (identity theft);
c) email scams set up to commit theft through banking
d) hacking: shutting down or misusing websites or computer networks;
e) spreading hate and inciting terrorism;
f) distributing child pornography;

4. Prevent Duty and Radicalisation

4.1. As we become a more digital society radical or extremist views become more accessible via the internet. Access to vulnerable individuals has become easier due to the increased use of social media. As a result the identifiers of someone becoming radicalised are similar to those of someone experiencing grooming.

4.2. Millions of young people use social media platforms every day to share content, but there are a growing number of users who exploit it to radicalise and recruit vulnerable people. The Internet has played a significant role in the radicalisation and recruitment of foreign fighters and continues to do so. Social networking is the main activity young people aged 16-24 use the internet for, something which extremist groups are well aware of using platforms such as Facebook, Twitter, WhatsApp and YouTube to draw young people to their cause.

4.3. Far-Right and Islamist extremist groups are using the Internet to recruit 'a new younger generation of members'. It is also facilitating the ability of extremist groups to organise and promote themselves.

4.4. There is a wealth of Far-Right and Islamic extremist material available online including; articles, images, videos encouraging hate or violence, posts on social media and, websites created or hosted by terrorist organisations. There are also terrorist training materials and videos glorifying war and violence that play on the theme of popular video games such as 'Call of Duty: Black Ops'. These use highly emotive language and images created to play on the issues young people are struggling with such as identity, faith and belonging.

5. Responsibilities

The following section outlines the broad online safety roles and responsibilities of individuals and groups within IBCM.

5.1. IBCM Board

5.1.1. IBCM Board, via the Executive Committee, is responsible for the overall effectiveness of the policy. This will be carried out by the Board receiving regular information about online safety

incidents and monitoring reports.

5.2. Designated Safeguarding Lead (DSL)

5.2.1. The DSL has a duty of care for ensuring safety within IBCM and therefore has overall responsibility for online safety within the organisation but will liaise with other members of staff as necessary.

5.2.2. The DSL will respond to online safety concerns reported in line with our safeguarding, Prevent, and other associated policies.

5.3. Users of IBCM ICT systems

5.3.1. Users of IBCM ICT systems include learners, customers and employees.

5.3.2. Users of IBCM ICT systems should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

5.3.3. Users are responsible for using IBCM IT systems in accordance with their IT user agreements and generally understanding the importance of adopting good online safety practice when using digital technologies in and out of the organisation.

5.4. Staff

5.4.1. Staff that work directly with customers and learners are also responsible for helping them understand the importance of online safety and how they can reduce exposing themselves to risk and unsuitable content which includes, but is not limited to, adult material, gambling, drugs, discrimination, racism, violence, child on child abuse, sexual violence and sexual harassment, terrorism and extremism.

5.4.2. Any reported incident of unacceptable conduct will be treated seriously and in line with other relevant policies and procedures.

5.5. ICT Technical Support

5.5.1. ICT support helps ensure that IBCM' technical infrastructure is secure and is not open to misuse or malicious attack. Appropriate filters, monitoring and password protection is in place to reduce the risk of online safety issues arising.

5.5.2. ICT support monitor usage of the internet through the installation of software on all company devices and through the network, allowing the team to monitor usage and users on the internet and restrict access to illegal, harmful or inappropriate images and content. Inappropriate use of internet will be reported through monitoring reports to the Safeguarding Lead.

6. Online Safety Procedures and Implementation

6.1. IBCM recognises that education in online safety is therefore an essential part of IBCM online safety provision. IBCM helps and supports young people and adults to recognise and avoid online safety risks and build their resilience through a combination of security measures, training, guidance and implementation of our policies.

6.2. IBCM will do all it can to make our customers, learners and staff stay safe online and to satisfy our wider duty of care. Online safety awareness will be embedded into everyday practice through:

- How to use technologies in a safe and responsible way
- Supporting and encouraging people to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Provide user agreements for use with staff and students

- Provide clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour
- Providing clear and specific directions on how to behave online (through a range of both student and staff facing policy and procedure documents).
- Reviewing and updating the security of our information systems regularly
- Ensuring that user names, logins, email accounts and passwords are used effectively
- Ensuring personal information about those who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of young people are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- Providing supervision, support and training about online safety
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

6.3. The IT Policy sets out the requirements in relation to appropriate use of technology and the internet and reporting unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, IBCM' Safeguarding Policy, and relevant procedures must be followed.

6.4. It is more likely that IBCM will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner and users will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through company behavior and disciplinary procedures.

7. Online Safety Training and Continuous Professional Development

7.1. All staff will receive training on company policies and procedures relating to safeguarding, Prevent and online safety and will be made aware of the local safeguarding arrangements as part of the company induction. Ongoing online safety training and updates for all staff, customer and learners will be integrated, aligned and considered as part of our overarching Prevent Duty and safeguarding approach.

7.2. All staff will be required to undertake online Prevent and Safeguarding training as part of their induction. This will be repeated on an annual basis.

7.3. All staff will have access to resources to support awareness of online safety through intranet, extranet and local resources.

7.4. IBCM will ensure a response is in place to enable all learners to learn about and manage online risks effectively as part of providing a balanced curriculum.

8. Remote delivery

8.1 As a result of the COVID-19 pandemic, remote delivery, assessment and invigilation has formed a part of the teaching and assessment practice at IBCM. This includes video recordings, Teams, Zoom, WhatsApp etc.

8.2 It is imperative that all safety procedures are followed during online delivery and that staff members are mindful of any potential risks.

8.3 Practitioners should ensure that the agreement part of the interaction takes place – even where the adviser has previously engaged with the customer – and that it is clear and understood. This should include basics on the core areas such as Safeguarding (confidentiality, disclosure), GDPR (recording) – as well as time of the interview and the ethics of a good interaction e.g. explore all options, be honest, ask questionsConsent must be obtained from all customers and recorded in the normal way.

8.4 Disclosure: students sometimes disclose information and emotion very quickly online. Tutors need to understand the dynamics underpinning this kind of response so that they can work effectively with students who exhibit this.

8.5 Risk Assessment: practitioners should assess each situation before the session and also pro-actively during the session to assess the risk to themselves and the young person and take action or change their approach accordingly.

8.6.1 Make sure the platform you are using is suitable. Also check the privacy settings so that it is secure as possible from outside hacking.

1.1. All practitioners and customers must wear suitable clothing, including anyone else in the household.

1.2. Any devices used should be in appropriate areas, for example, not in bedrooms. Consider the background that the customer will see on video.

1.3. Language must be professional and appropriate, including that of any family members in the room.

1.4. Webinars and live broadcast should be recorded where possible to maintain a record of the activity. You will need to store this in line with GDPR requirements. This is possible in teams and some apps, further guidance will follow.

9. Policy Monitoring and Evaluation

9.1. The Executive Committee will conduct an annual review of our online safety systems and policies. This will include consideration of specific cases dealt with by staff in the last year. The resulting information, including feedback from staff, will be used by the designated person to inform any improvements necessary. Quarterly online safety reports will be reviewed at IBCM Board level.

9.2. IBCM online safety policy and procedures will be clearly communicated to staff, learners, subcontractors, Board Members and Service Users through the use of the company intranet and extranet. The Designated Safeguarding Officer will be responsible for ensuring this is done.

10. Designated Safeguarding Team Contacts:

Designated Lead for Safeguarding – Rachena Kumari, Principal
Mob: 07881028058
Email: principal@ibc-manchester.com

11. Related Policies

This policy should be read in conjunction with:

IBCM Prevent Policy
IBCM Safeguarding Policy
IBCM IT Policy
IBCM User Agreements
IBCM Bullying and Harassment Policy
IBCM Staff Handbook
IBCM Student charter

Annex 1 Guidance on Responding to Online Safety Incidents

Do not share information about the incident with anyone but DSL (inc. parents/carers)

Do not blame and shame

Do explain it needs to be reported and the person will get support.

An online safety issue is identified/reported
Establish the severity of the incident

Never view, copy, print share, store or save any imagery yourself or ask anyone to share or download.This is illegal.

If you have already viewed by accident report this to the DSL,

Do not delete or ask the young person to delete the image(s)

Is the material accessed or the action performed illegal?

No

Yes

Report the incident to the relevant person depending on the severity of the incident:

DSL
Managing Director

What risk is posed to the user involved?

Report the incident to the relevant person depending on the severity of the incident:

DSL
Managing Director
Relevant Authorities

Responses to the incident as appropriate:

- Websites blocked
- Any inappropriate content submitted by user is evidenced and removed
- Warning/sanctions are given to the user if appropriate
- Review any learning from incident and amend processes and/or online safety policy.
- Implement any changes in order to minimise reoccurrence of the incident
- Record steps taken to resolve the issue
- Monitor the situation for any potential developments/recurrences, particularly relevant to online abuse.
- If needed provide report and evidence to relevant authority
- Review training on online learning for user/ company as necessary and update.

If an immediate risk

- Secure and preserve all evidence and hardware (do not send on materials)
- Report to Designated Safeguarding Officer
- DSL to report to Social Care team/police as immediate danger.
- Allow the authorities to complete their investigation and take the necessary steps once it has been concluded.

If no immediate risk

- DSL to report the incident to the police /child exploitation and online protection unit (CEOP) / Internet Watch Foundation (IWF) / Social Care as appropriate.
- Allow the authorities to complete their investigation and take the necessary steps once it has been concluded.

RELATED POLICES
Please also refer to Supplementary Policies:

- Prevent and Safeguarding Policy
- Staff Handbook
-

VERSION CONTROL

Version	2.0
Originator	M.D.
Effective from	July 2024
Approved by	Board of Governors
Review Date:	July 2025