Weston College Group

# E-Safety & Social Media Policy

# E-Safety & Social Media Policy

## CONTENTS

# E-Safety & Social Media Policy

**Change Control**

| | |
|---|---|
| **Version:** | 3.2 |
| **Date approved by CLB:** | July 2023 |
| **Date approved by Corporation:** | N/a – authority for approval of operational policy delegated to CLB |
| **Name of the policyholder:** | Jon Hofgartner |
| **Date issued:** | July 2023 |
| **Review date:** | January 2025 |

| Version | Type – New/Replacement/Review | Date | History |
|---|---|---|---|
| 3.0 | Replacement | 22/01/2021 | Reviewed and updated document template |
| 3.1 | Review | 20/10/2021 | Minor mod to section 5 to more clearly articulate the issue of 'online sexual abuse and harassment' within e-safety. |
| 3.2 | Review | 09/08/2023 | Minor mods only |

This policy applies to Weston College Group and all wholly-owned subsidiary companies of the Weston College Corporation which include OLASS, Forward Futures, SOMAX, Releasing New Potential, Inspirational Events and Investments

# E-Safety & Social Media Policy

## 1 PURPOSE

1.1 Weston College recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

1.2 Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

1.3 This policy must be read in conjunction with other relevant College policies including Safeguarding of Children & Adults at Risk Policy, IT Acceptable Use Policy, Anti Bullying and Harassment (Learners and Staff), Learner Disciplinary and Code of Conduct and the Staff Disciplinary and Dismissal Procedures.

## 2 SCOPE

2.1 This policy covers:

- Anyone representing Weston College Group
- Anyone logging into any network, service, website or portal associated with Weston College.
- Connecting a device via the Weston College network.
- Any electronic communication with a Weston College Learner, member of Staff or contractor.
- From any geographic location both on Campus and off Campus.

## 3 MONITORING USAGE

3.1 The Weston College Group activity monitor, log and report on learners and staff use of IT systems and IT network usage as part of the College's responsibility towards the 'safeguarding of young people and vulnerable adults' and Prevent duty for terrorist and extremist behaviour.

3.2 An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the College's disciplinary process.

3.3 Any use of College resources or online communication considered to be unlawful will be reported and shared with the Police for further investigation

3.4 All personally identifiable information is collected, stored, processed and shared following the Weston College Group Privacy Policy available from www.weston.ac.uk/dataprivacy

## 4 CYBERSECURITY

4.1 Weston College IT systems and the College's Information Security Management System is certified to meet the following Information Security and Cyber Security standards:

- Cyber Essentials (registration number QGCE1054)
- ISO 27001 – Information Security (certificate number IS656993)

4.2 These standards are regularly reviewed by independent experts providing staff, learners & stakeholders reassurance that Weston College IT systems cybersecurity follow the highest levels of best practice.

4.3 Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring/accessing someone else's digital identity is a criminal offence and will be referred to the college's disciplinary procedure and sent to the police for investigation.

4.4 If you have any concerns or notice anything suspicious in regards to the cybersecurity of the Weston College network or systems please contact the IT Helpdesk on 01934 411425 or it.helpdesk@weston.ac.uk

## 5 TRAINING & GUIDANCE

### Learners

5.1 E-safety guidance is provided by personal tutors and learners can access e-safety resources from the MyWeston homepage and VLE resources.

5.2 Tutorial planning includes appropriate and relevant e-safety guidance for learners, including online sexual abuse and harassment.

5.3 The MyWeston homepage will include online guidance for safeguarding, including how to report concerns and key definitions for sexual abuse and harassment.

5.4 The Individual Development (ID) programme for full-time learners ensures learners consider their digital footprint in both a personal and professional context.

5.5 Online learning for staying safe online and digital citizenship is accessible through the induction modules and group tutorial online resources.

5.6 Learners will receive guidance on what precautions and safeguards are appropriate when making use of specific the internet and mobile technologies from their curriculum tutor.

5.7 If learners have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. They must report this to their tutor

5.8 Learners will be prompted with a reminder of the Colleges IT Acceptable Use Policy each time they log in to a Weston College Computer

5.9 The college e-safety expectations and e-safety themes will be highlighted within tutorial and awareness campaigns throughout the academic year.

5.10 Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded.

5.11 Learners are required to respect the copyright of other parties and to cite references properly.

### Staff

5.12 Staff will receive an introductory session for digital learning/working systems and environments within the induction period.

5.13 This introductory session will signpost the E-Safety Policy and provide an overview for academic staff.

5.14 Staff are required to attend annual safeguarding training, including update training, to maintain an understanding and awareness of online sexual abuse and harassment.

5.15 A formal agreement to the expectations and terms will be managed by the Human Resources department. Each member of staff must record the date of the training attended on their CPD calendar.

## 6 BEHAVIOUR

6.1 Use of any Weston College IT equipment and systems is conditional to the College Policies including the IT Acceptable Use Policy & the Anti-Bullying Harassment Policy and Procedure.

6.2 When in a position or situation where your views may be associated with the Weston College Group you must not link yourself with views which may bring the College into disrepute. This includes social media "likes" and or comments

6.3 Communications by staff and learners must always be courteous and respectful 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).

### Cyberbullying

6.4 Cyberbullying is a form of bullying. As it takes place online, it is not confined to college buildings or college hours. Cyberbullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

6.5 Cyberbullying 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.

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

## 7 SAFEGUARDING & PREVENT

7.1 Staff must be aware of the College's responsibility for the Prevent Duty and Safeguarding of young people and adults at risk.

7.2 Staff must understand the risk to young people and adults of online sexual abuse and harassment, including appropriate safeguarding procedures to respond to concerns.

7.3 Where staff encounter or suspect online sexual abuse or harassment, staff should follow the College's referral process for safeguarding concerns.

7.4 The following guidelines must be adhered by all staff communicating online:

- Staff must not post or associate themselves with any personal views, beliefs or opinions which undermine British Values or may put someone's safety at risk
- Staff must challenge any personal views, beliefs or opinions posted by learners which undermine British Values or may put someone's safety at risk
- Staff must post 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 must be referred to a Safeguarding Officer for further investigation
- Any post considered to promote extreme views must be referred to a Safeguarding Officer for further investigation

## 8 ONLINE COMMUNICATION

8.1 The appropriate use of online communication applies to all devices and services, which might include:

- Computers, Laptops & Mobile devices (including phones and tablets)
- Game Consoles
- Email, Instant / Direct Messages & Chat rooms
- Social Media

8.2 When using any online communication technology, you must:

- Be concise
- Be engaging and use appropriate language
- Use decent-quality images whenever possible
- Use British English, correct spelling and grammar
- Follow the appropriate style and brand guidelines.

8.3 All online communication which may be associated with the Weston College Group must be professional.

8.4 Inappropriate use of online communication will be referred to the Colleges disciplinary procedure.

8.5 Any online communication considered to be a criminal offence will be referred to the police for investigation.

8.6 You must not create, redistribute, support (like) or download any message, media or content which may cause offend or be considered harassment.

8.7 You must report any message, media or content which may cause offence or be considered harassment to your tutor or a responsible adult.

8.8 You must not send messages at random or excessively, also referred to as "spamming".

8.9 You must not make or receive personal calls, messages or emails etc. whilst in a teaching environment.

8.10 You must portray a balanced tone when raising politically sensitive issues.

### Staff Communicating with Learners

8.11 Staff must not communicate with learners from non-College accounts or personal phone numbers

8.12 Staff must not give personal contact details to learners.

8.13 Staff must not communicate with learners from non-College accounts or personal phone numbers

8.14 Staff must not give personal contact details to learners.

8.15 Learner contact details must never be stored on a staff members' personal device(s), including computers, laptops, mobile phones, tablets, personal cloud or personal storage devices.

8.16 When linking to online resources not controlled by the Weston College Group (such as to relevant news articles) it must be clear that the link is external

8.17 Only approved online messaging services can be used to communicate with learners, all communication must be via a College user account these include

- Email (using a college account)
- Skype for Business (using a college account)
- Microsoft Teams and Microsoft Office 365 collaboration (using a college account)
- SMS (using a College device)

8.18 The use of any other communication application including but not limited to Snapchat, Facetime, iMessage & WhatsApp are not permitted to communicate with learners.

## 9 SOCIAL MEDIA

### Use of Weston College social media accounts

9.1 Only employees who have been authorised to use social media accounts through the College Group's social media approval process may access social media on the College Group network or create, maintain, or post on behalf of official College Group accounts.

9.2 The use of social media will only be approved where it is deemed to benefit learners and learning, is in the business interests of the College, and meets safeguarding and PREVENT duties.

9.3 The College Group has several official social media communications channels, which are part of the College Group infrastructure. These take priority in externally published documents and materials.

9.4 In the event of an incident or emergency involving Weston College Group, Information regarding the incident must only be by the Marketing and Communications team who will manage PR centrally

### Creating new social media accounts

9.5 New social media accounts that use an official logo or a Weston College Group name must not be created unless approved through the social media approval process.

9.6 The Marketing and Communications Department and Lead Safeguarding Officer must be given administrator access to social media accounts which appear to represent the College Group or an aspect of its provision.

9.7 In addition to this, all social media accounts must be accessible by a second administrator at all times. When an administrator leaves the College Group, their access to College Group social media accounts must be revoked, and the account either handed over to another administrator or closed.

9.8 The College will close down any “unofficial” social media sites using the Colleges logo, name or copyrighted materials, even if created by staff or learners.

## Social media privacy settings

9.9 College Group employees must be aware of their social media presence, particularly when the social media account openly states that they work within the College Group.

9.10 Your social media presence on sites such as Facebook can contain a lot of personal information that you might not wish to share with your colleagues, employer or the general public.

9.11 Unless your privacy settings are restricted, your colleagues, employers and learners may be able to access your personal information. Therefore, it is important to ensure that your privacy settings reflect the amount of information you want people to find out about you.

9.12 On Facebook, in particular, there are many settings which can be altered to automatically restrict people’s access to your profile; however, your cover image, name and profile pictures can be viewed by anyone with access to the site. Employees must ensure that their Facebook content and posts are restricted to people in their friend's list.

9.13 It is recommended that other staff personal profiles are set to the maximum possible security settings. This means that only you and people in your friends and/or followers list will be able to see the updates you post.

9.14 Members of staff are responsible for managing their own social media presence and ensuring that their privacy settings are correct. Staff members are responsible for ensuring that their privacy settings are appropriate for the type of content they share on social media.

## Accepting friends/followers

9.15 Employees of the Weston College Group must maintain professional boundaries at all times, particularly when accepting or inviting ‘friend’ connections on personal social media accounts.

9.16 Employees must not passively or actively connect on social media with current or ex-learners who are under the age of 18 or who have a vulnerability, adult learners who they teach, support or could be deemed to give an unfair advantage to, or any other persons deemed inappropriate by the Lead Safeguarding Officer.

9.17 People who studied within the College Group when they were under the age of 18 must not be added as connections by members of staff until five years after they have left the Weston College Group.

9.18 Entering into such relationships may lead to abuse of an employee’s position of trust and breach the standards of professional behaviour and conduct expected at the College Group. The College Group reserves the right to take disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

9.19 Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Adult and Children Board and/or the Independent Safeguarding Authority.

9.20 Exceptions to this rule can be made when the primary connection between an employee and a restricted person does not stem from them being a learner of, or from interactions within, the College Group, and this has been declared as an expression of interest to the Lead Safeguarding Officer. This includes instances in which an apprentice in the College Group’s employment connects with their peers who study within another aspect of the Group’s provision.

9.21 When the social media account uses a passive connection, such as the 'follow' action on Twitter and Instagram, employees must not 'follow' learners or ex-learners under the age of 18. If a learner or ex-learner under the age of 18 'follows' a College Group employee, the employee must be aware that the person may be able to access private information and images shared by the employee.

### Using social media in the employee recruitment process

9.22 The Weston College Group may view relevant social media websites as part of the pre-employment process, i.e. those specifically aimed at the professional market and used for networking and career development such as LinkedIn.

9.23 Any information which relates to the applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

### The social medial approval process

9.24 All employees who want access to view, create or maintain social media accounts must have read this policy and completed the necessary acknowledgement form.

9.25 The social media approval form is kept in the Policy & Procedures section of SharePoint. Each section of the form must be filled in before submission.

9.26 The completed form is then reviewed by the Lead Safeguarding Officer, who considers the safeguarding and PREVENT implications of the social media account.

9.27 If the social media account is approved by the Lead Safeguarding Officer, the form is sent to the Digital and Creative Manager, who will either approve or reject the form after considering the marketing implications of the social media account and its relation to the College Group's social media and marketing strategy.

9.28 If both the Lead Safeguarding Officer and the Digital and Creative Manager approve the application, it will pass to IT Helpdesk who will provide the user with access to social media via group policy, on their work devices.

### Social Media in Teaching and Learning

9.29 Social media can help in reaching learners to inform them of course-related activities, events and news. Social media can be used to enhance a learner's experience through carefully planned use in teaching and learning, however social media platforms must not be the primary learning environment for learners.

9.30 Course content, collaborative working, group discussion and class level communication must be based within the agreed College learning and working environments. For teaching and learning, Microsoft Teams, SharePoint and the VLE are the College's chosen digital learning and working environments.

9.31 All learners will have a Weston College IT account, providing access to these digital learning and working environments. Internal technical support, guidance and training are also available to users of these platforms through IT helpdesk, LibraryPlus and Learning Technologists.

9.32 Learners are not obliged to create social media accounts to access course materials and learners must not be disadvantaged by choosing not to participate within a social media platform.

## 10 WEB CONFERENCING, REMOTE TEACHING & LEARNER SUPPORT

10.1 The following protocols must be adhered to when using web conferencing for online group sessions or one-to-one sessions.

### Groups Sessions – Staff Must

10.2 Be up to date on all safeguarding training and ensure they are familiar with the e-safety policy.

10.3 Only use video conferencing tools supported by Weston College using staff and learner accounts (Microsoft Teams).

10.4 Record sessions with learners (both one-to-one and group delivery). This is helpful for learners to refer to and to provide support if any issues arise.

10.5 Notify learners that the meeting is being recorded and may be shared internally if required.

10.6 Communicate appropriate location, dress and conduct for learners to participate in both group and one-to-one online sessions (ready to learn).

10.7 Ensure regular sessions are pre-scheduled through the Microsoft Teams calendar.

10.8 Report concerns to your line manager and/or safeguarding officer as soon as possible if feeling uncomfortable with something said or done during a group session.

10.9 Remain professional throughout the meeting as a representative of the organisation.

10.10 Conduct video conferencing from a desk or other appropriate location.

10.11 Be mindful of appearance on camera; focus on the screen, pay attention to participants and look at the camera when speaking.

10.12 Use background effects where possible.

10.13 Be aware of surroundings and what might be visible to others on the call.

10.14 Preview your video before the call.

10.15 Be appropriately dressed in work-appropriate wear at all times.

10.16 Mute microphones when not talking to avoid background noise.

10.17 Keep online sessions and meetings to a reasonable duration, being mindful of screen breaks.

### Groups Sessions – Staff Must Not

10.18 Conduct a video conference if it would be inappropriate to meet face-to-face (e.g. out of hours, weekends etc.).

10.19 Use video conferencing tools/platforms that are not supported by Weston College and/or use personal accounts/email addresses.

10.20 Use private messaging apps with learners for one-to-one discussions/meetings.

10.21 Be positioned where background activities and other people may be seen in the video conference.

### One-to-one Sessions – Staff Must

10.22 Facilitate one-to-one meetings with learners only within Microsoft Teams using Weston College / UCW user accounts.

10.23 Check the faculty has informed parents/carers that online one-to-one sessions may be required as part of tutorial and learner support service activities.

10.24 Ensure one-to-one sessions with vulnerable learners have been agreed with parents/carers before scheduling.

10.25 Ensure any one-to-ones with vulnerable learners take place only at the days/times agreed with parents/carers and are pre-scheduled through Microsoft Teams.

10.26 Record all one-to-one sessions with learners using Microsoft Teams if any issues arise. This is also helpful for learners to refer back to.

10.27 Notify learners that the one-to-one meeting is being recorded and will not be routinely shared.

10.28 Consider whether another staff member should join a one-to-one meeting with a learner (e.g. support worker).

10.29 Agree on protocols and timings of all one-to-one online activity with learners.

10.30 End the call immediately if feeling uncomfortable with something said or done during a one-to-one meeting and report concerns to your line manager and/or safeguarding officer.

### One-to-one Sessions – Staff Must Not

10.31 Conduct a one-to-one video conference if it would be inappropriate to meet face-to-face (e.g. out of hours, weekends etc.).

10.32 Move/extend one-to-one messaging or calls into social messaging apps and/or social media platforms.

## 11 DIGITAL HEALTH & WELLBEING

11.1 The digital tools and platforms available to staff and learners provide a high level of connectivity through mobile apps, web services and integrations. Staff and learners must be mindful of the health and wellbeing of others when frequently using these technologies outside of normal working hours.

11.2 Staff must set communication expectations including digital etiquette with learners. This must form part of the induction period and/or when introducing Microsoft Teams, email or other approved communication platforms to learners.

## 12 COPYRIGHT

12.1 Staff and learners are responsible for ensuring they have the appropriate copyright licence for the use of any content or media being used.

12.2 All copyrighted material must be obtained from a legitimate licensed source.

12.3 The distribution of material which infringes copyright is a criminal offence and will be referred to the College's disciplinary process and/or the police for investigation

12.4 The use of file-sharing software including but not limited to BitTorrent is forbidden over the College network

12.5 The use of any website must be used within accordance with the website terms and conditions

12.6 The downloading of YouTube videos for offline use is not permitted by the terms and conditions of the website.

12.7 Copyright guidance for learning resources is available through the Head of Learning Centres.

## 13 PRIVACY OF PERSONAL INFORMATION

13.1 Staff must not request any information that relates to an identified or identifiable living individual unless this has been approved by the Weston College Groups Data Protection Officer or Data Privacy Team

13.2 Before any information that relates to an identified or identifiable living, individual is requested an appropriate Privacy Notice will be provided detailing how the information will be processed and what rights the individual has.

13.3 All personally identifiable information will be collected, stored, processed and shared following appropriate laws and best practice.

13.4 Staff personal devices must not be used to take photos or record videos of learners

13.5 College devices can be used to take photos or record videos of learners, all media files must be stored on support College systems (Network Storage/ Office 365) only

13.6 All photos and videos containing personally identifiable information must be processed following the Colleges Privacy Policy and legal requirements

## 14 FEEDBACK & FURTHER INFORMATION

14.1 Weston College welcomes all constructive feedback on this and any other college policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact: Fiona Waters, Safeguarding Officer

### Useful Links for further information:

Digital You! – Weston College Student Zone
https://weston.sharepoint.com/sites/WC_StudentSharePoint/SitePages/Digital-You!.aspx

Child Exploitation & Online Protection Centre
http://www.ceop.police.uk/

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

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

## 15 RESPONSIBILITIES

15.1 The reporting responsibilities for e-safety follow the same lines of responsibility as the College Safeguarding.

**All Staff & Workforce**

- Responsible for ensuring the safety of learners
- MUST report any concerns or disclosures immediately to a First Response Officer (FSO) or Designated Safeguarding Officer (DSO)

- 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 e-safety and display a model example to learners at all times.
- MUST actively promote through embedded good e-safety practice.
- MUST communicate with learners professionally and in line with the college Communications Policy at all times.

**Learners**

- MUST keep to the terms and conditions of the IT Acceptable Use Policy at all times
- Must receive appropriate e-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 member of the college community.
- Learners must act safely and responsibly at all times when using the internet and/or mobile technologies.

**Safeguarding Officers (FSO / DSO)**

- MUST follow the safeguarding Reporting Procedure in Appendix A at all times
- With management, approval refers to appropriate additional support from external agencies.

**Safeguarding Leads**

- Leading the Safeguarding Committee
- 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 e-safety within the College community.

**IT Department**

- Ensure the College's 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 e-safety concerns or disclosures immediately to a First Response Officer (FSO) or Designated Safeguarding Officers (DSO)

## Records management

15.2 Staff must maintain all records relevant to administering this policy using the ISMS Control of Information Assets Procedure (WCGIT-1214890995-8).

# 16 RELATED LEGISLATION AND DOCUMENTS

## Legislation & Regulation

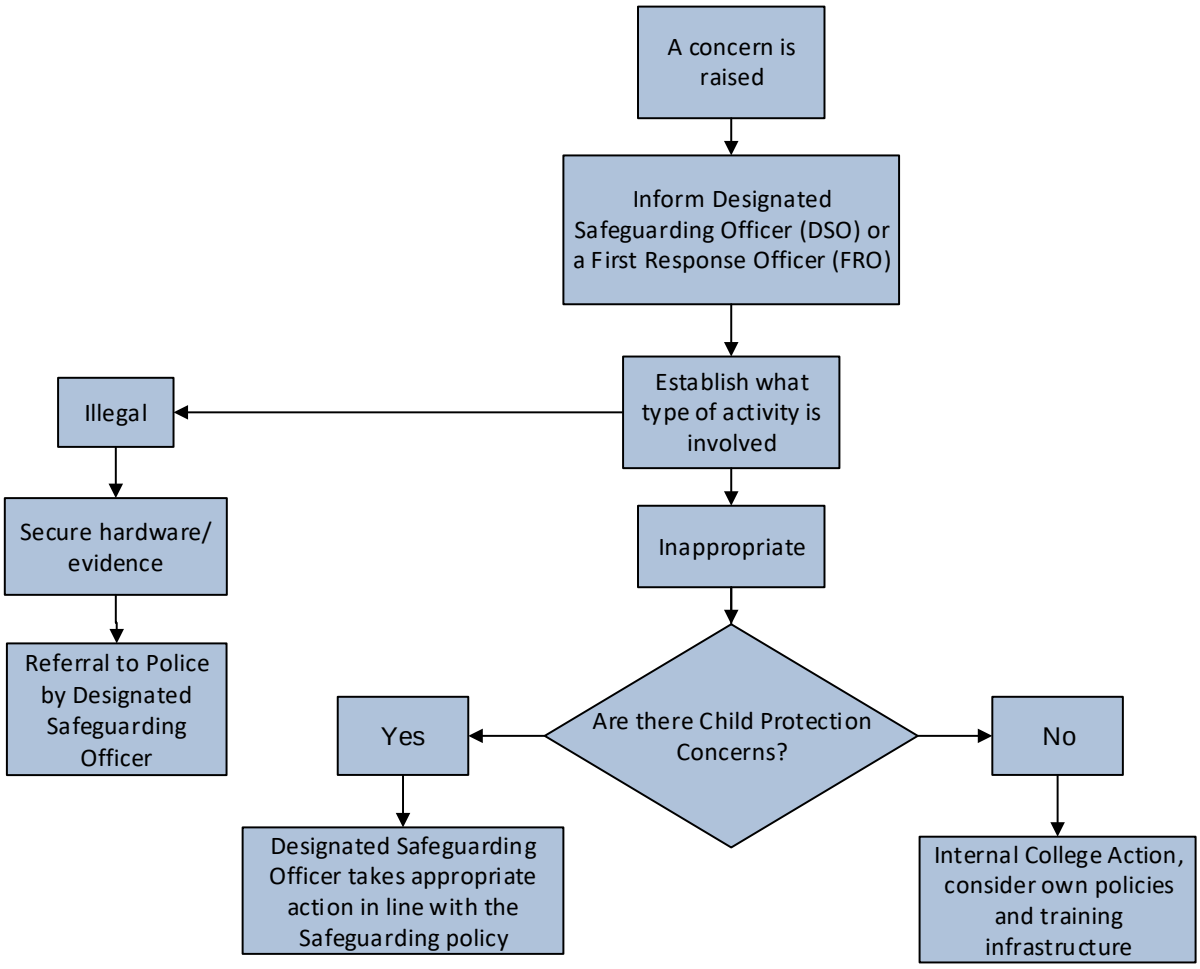
Copyright, Designs and Patents Act 1988
Computer Misuse Act 1990

Data Protection Act 2018
General Data Protection Regulation (EU) 2016
ISO/IEC 27001:2013 Information Security

## Other Policies & Procedures

Anti Bullying and Harassment (Learners and Staff)
Information Security Policy (WCGIT-1214890995-12)
ISMS Control of Information Assets Procedure (WCGIT-1214890995-8)
IT Acceptable Use Policy (WCGIT-535199308-3)
Learner Disciplinary and Code of Conduct
Safeguarding of Children & Adults at Risk Policy,
Staff Disciplinary and Dismissal Procedure

## 17 APPENDIX A – INCIDENT MANAGEMENT PROCESS



## 18 APPENDIX B – MICROSOFT TEAMS GUIDANCE

Microsoft Teams is a powerful collaborative working and communication tool available within the Microsoft Office 365 environment. Microsoft Teams is a key digital learning and working platform for many staff and learners at the College. Below is a list of guidelines for using Microsoft Teams:

- Ensure you are confident in using the application by attending training with a Learning Technologist.

- Microsoft Teams as a platform is used for teaching, learning and assessment with several specific features for educators.

- Understand how Microsoft Teams is used within your department/faculty.

- Introduce learners to their Microsoft Team as part of their induction, making sure to frame the use and set expectations, for example:

    - Teams communication is for course-related content, discussion and support only
    - Appropriate College communication channels should be used for safeguarding and welfare queries, questions and/or disclosures
    - Conduct within Teams should be professional and courteous
    - Offensive and inappropriate conduct will be subject to College disciplinary procedures
    - Communication should follow the expectations set out within the Social Media Policy
    - Staff are not expected to respond to Microsoft Teams communication outside of working hours
    - Staff and learners are not obliged to download the Microsoft Teams app on personal devices, however, this can be beneficial to both.

- Chat logs from both one-to-one and group chats can be provided by IT in the event of misconduct or a complaint.

- Microsoft Teams is not a 'Virtual Learning Environment' (VLE) but does have a range of functionality for teaching, learning and assessment. Staff development and curriculum design must be considered when adopting Microsoft Teams. For time-specific or structured online learning, staff should consider using a VLE or external resources that have been procured through the College. Contact learningtech@weston.ac.uk for further guidance.

For any further guidance, training and support for Microsoft Teams, please contact learningtech@weston.ac.uk. The Learning Technology SharePoint page includes a range of support materials and training.

Staff and learners can also access online training for a range of Microsoft applications, including Teams, through the Microsoft Educator Community (https://education.microsoft.com/)

# 19 APPENDIX C – SOCIAL MEDIA NCSC GUIDANCE

The National Cyber Security Centre (NCSC) part of HM Governments GCHQ have released guidance on the safe use of Social media in their Social Media: how to use it safely post. Below is an excerpt of this document.

## Advice from social media platforms

The following guidance is provided by each of the major social media platforms. Click to read detailed information.

- Facebook: basic privacy settings and tools
- Twitter: how to protect and unprotect your Tweets
- YouTube: privacy and safety
- Instagram: privacy settings and information
- LinkedIn: account and privacy settings overview
- Snapchat: privacy settings

## Use two-factor authentication (2FA) to protect your accounts

Two-factor authentication (often shortened to 2FA) provides a way of 'double-checking' that you are the person you are claiming to be when you're using online services, such as social media, banking or email. Even if a criminal (or someone simply looking to cause mischief) knows your password, they won't be able to access any of your accounts that are protected using 2FA.

- Facebook: How to Turn on 2FA
- Twitter: How to Turn on 2FA
- YouTube: How to Turn on 2FA
- Instagram: How to Turn on 2FA
- LinkedIn: How to Turn on 2FA
- Snapchat: How to Turn on 2FA

For more information on why you should use 2FA wherever you can, read the NCSC's official guidance on two-factor authentication.

## Understanding your digital footprint

It's worth exercising some caution when using social media. Not everyone using social media is necessarily who they say they are. Take a moment to check if you know the person, and if the friend/link/follow is genuine.

Less obviously, you should think about your digital footprint, which is a term used to describe the entirety of the information that you post online, including photos and status updates. Criminals can use this publicly available information to steal your identity or use it to make phishing messages more convincing. You should:

- Think about what you're posting, and who has access to it. Have you configured the privacy options so that it's only accessible to the people you want to see it?

- Consider what your followers and friends need to know, and what detail is unnecessary (but could be useful for criminals).

- Have an idea about what your friends, colleagues or other contacts say about you online.

Although aimed at businesses, CPNI's Digital Footprint Campaign contains a range of useful materials (including posters and booklets) to help understand the impact of your digital footprint.

## Social media and children

Most social media accounts require users to be at least 13 years old. However, it is easy to sign-up with a false date of birth. For expert advice about how to keep children safe online, please refer to:

- Thinkuknow: National Crime Agency: education programme for children
- Internet Matters.Org: Social Media Tips
- NSPCC: keep your child safe on social networks