
# E-Safety & Social Media Policy

# 1.0 Introduction

Weston College recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order 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.

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.

This E-Safety policy should 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 (Students and Staff), Student Disciplinary and Code of Conduct and the Staff Disciplinary and Dismissal Procedures.

## 1.1 Scope

This policy covers:

- 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.

# 2.0 Responsibilities

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

**All Staff**

- 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.

**Learner:**

- 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 1 at all times
- With management approval refer to appropriate additional support from external agencies.

**Safeguarding Lead**

- 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 Colleges 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)

Any extension of this policy will require the express written permission of the Corporate Leadership Board.

# 3.0 Monitoring

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.

An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the Colleges disciplinary process.

Where requested this information will be securely shared with appropriate local authorities and external support agencies.

# 4.0 Cyber Security

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

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

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

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 colleges disciplinary procedure and sent to the police for investigation.

# 5.0 Training

**Learners:**
Learners will be provided with e-safety guidance by personal tutors and have access to e-safety information on the Student Zone intranet. Tutorial planning will include appropriate and relevant e-safety guidance for learners. Tutorial and the L3 'Futures Academy' programme will also ensure learners consider their digital footprint in both a personal and professional context.

Issues associated with E-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. A link to the college e-safety expectations will appear when users log on to the college network as well as highlighting e-safety themes within tutorial and awareness campaigns throughout the academic year.

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.

**For staff:**
Staff will receive an introductory session for digital learning/working systems and environments within the induction period. This introductory session will signpost the E-Safety Policy and provide an overview for academic staff. 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.
Any new or temporary users will also be asked to sign the college Staff IT Policy.

# 6.0 Behaviour

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.

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 students).

**Cyber Bullying**
Cyber bullying is a form of bullying. As it takes place online, it is not confined to college buildings or college 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, 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.

# 7.0 Safeguarding & Prevent

Staff should beware of the Colleges 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 Safeguarding Officer for further investigation

# 8.0 Online Communication

**Online communication 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

**GDPR**

Before contacting any individual, you must have a “Lawful basis for processing” the contact information.

For more information refer to https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

**Do’s and Don’t**

The points below offer guidance on appropriate use of online communication.
Any breach of this guidance will be referred to the Colleges disciplinary procedure.
Any breach considered to be a criminal offence will be referred to the police for investigation.

The appropriate use of 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

1. You must not create, store, exchange, display, print or circulate any message or media which may cause offense to others.
2. You must not post or circulate any message which may be considered harassment.
3. You must not send messages at random or excessively, also referred to as "spamming".
4. Staff must not use personal devices or accounts as a method of communicating with students.
5. Staff must not give personal contact details to students.
6. Student contact details must never be stored on a staff members' personal device(s), including computers, laptops, mobile phones, tables, personal cloud or personal storage devices.
7. Staff and students must not make or receive personal calls, messages or emails etc. whilst in a teaching environment.
8. College devices may, on occasion, be used to gather either video or photographic evidence in order to support students' course requirements provided that the college hold a signed authorisation form for the student in question. All personal images will be held in accordance with the Colleges Privacy Statement.
9. You must not give out any personal information such as contact details, financial information or passwords (however this is not an extensive list).
10. You should not open files or emails from people you do not know. They may contain viruses or offensive material.
11. If you see something abusive or upsetting online, you must report it to a trusted adult.
12. You should not save your log-on details on shared computers as some people may use your screen name to defraud or scam people in your contact lists.
13. There may be legal implications if the Internet is used for criminal intensions for example to intimidate or to extract financial information for personal gain. All conversations using college IT systems are captured and recorded on the college's servers.
14. You must not post any confidential information to any online platform.
15. You must own the copyright of any material you post

If your post could be considered as representing or being associated to the College in any way then:

- It is imperative to portray a balanced tone when raising politically sensitive issues.
- When linking to websites not controlled by the Weston College Group (such as to relevant news articles) it must be clear that the link is external

No communication should be made with learners from personally created user accounts or phone numbers.

Only approved online messaging services can be used to communicate with students, 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)
- iMessenger (using a College device and account)
- SMS (using a College device)

The use of any other communication application including but not limited to SnapChat & WhatsApp are <u>not</u> permitted to communicate with students.

# 9.0 Social Media

**Use of Weston College social media accounts**

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.

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.

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

In the event of an incident or emergency involving Weston College Group no content should be posted to any social media channels except by the Marketing and Communications team who will manage PR centrally

**Creating new social media accounts**

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.

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.

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.

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

**Online privacy and personal information**

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.

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.

Unless your privacy settings are restricted, your colleagues, employers and students 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.

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 are able to be viewed by anyone with access to the site. Employees must ensure that their Facebook content and posts are restricted to people in their friends list.

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.

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.

## College Reputation

College Group employees and learners are expected to respect the Colleges reputation when posting online.

Any information which may be consider damaging the Colleges reputation may result in disciplinary and/or legal action

Use of the Colleges Intellectual Property (IP) must be requested and approved by the Marketing department. Any use of IP without permission may result in disciplinary and/or legal action.

## Accepting friends/followers

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.

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

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.

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.

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.

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 student 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.

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-students under the age of 18. In the event that a student or ex-student 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.

If an employee becomes aware of a student under 18 or a vulnerable adult who has 'followed' those, employees must block them.

**Using social media in the employee recruitment process**

The 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. 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.

**Social medial approval process**

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

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.

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

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.

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**

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.

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 and Canvas (TIDE) are the College's chosen digital learning and working environments.

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, Library Plus and Learning Technologists.

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

# 10.0 Copyright

- Staff and Students are responsible for ensuring they have the appropriate copyright licence for the use of any content or media being used.
- All copyrighted material must be obtained from a legitimate licensed source.
- The distribution of material which infringes copyright is a criminal offence and will be referred to the Colleges disciplinary process and/or the police for investigation
- The use of file sharing software including but not limited to Bit torrent is forbidden over the College network
- The use of any website must be used within accordance of the website terms and conditions
- The downloading of YouTube videos for offline use is not permitted by the terms and conditions of the website.
- Copyright guidance for learning resources is available through the Library Plus Manager.

# 11.0 Use of Images & Video

Where the College has 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 College 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 the College premises should be considered carefully and have the consent of both the Corporate Management Team / Marketing Department before being published. Approved photographs should not include names of individuals.

# 12.0 Personal Information

Personal information will be held and processed in accordance with the General Data Protection Regulation (GDPR) 2018.

For more information please refer to the Weston College Privacy Statement available on the website www.weston.ac.uk

# 13.0 Feedback and Further Information

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:

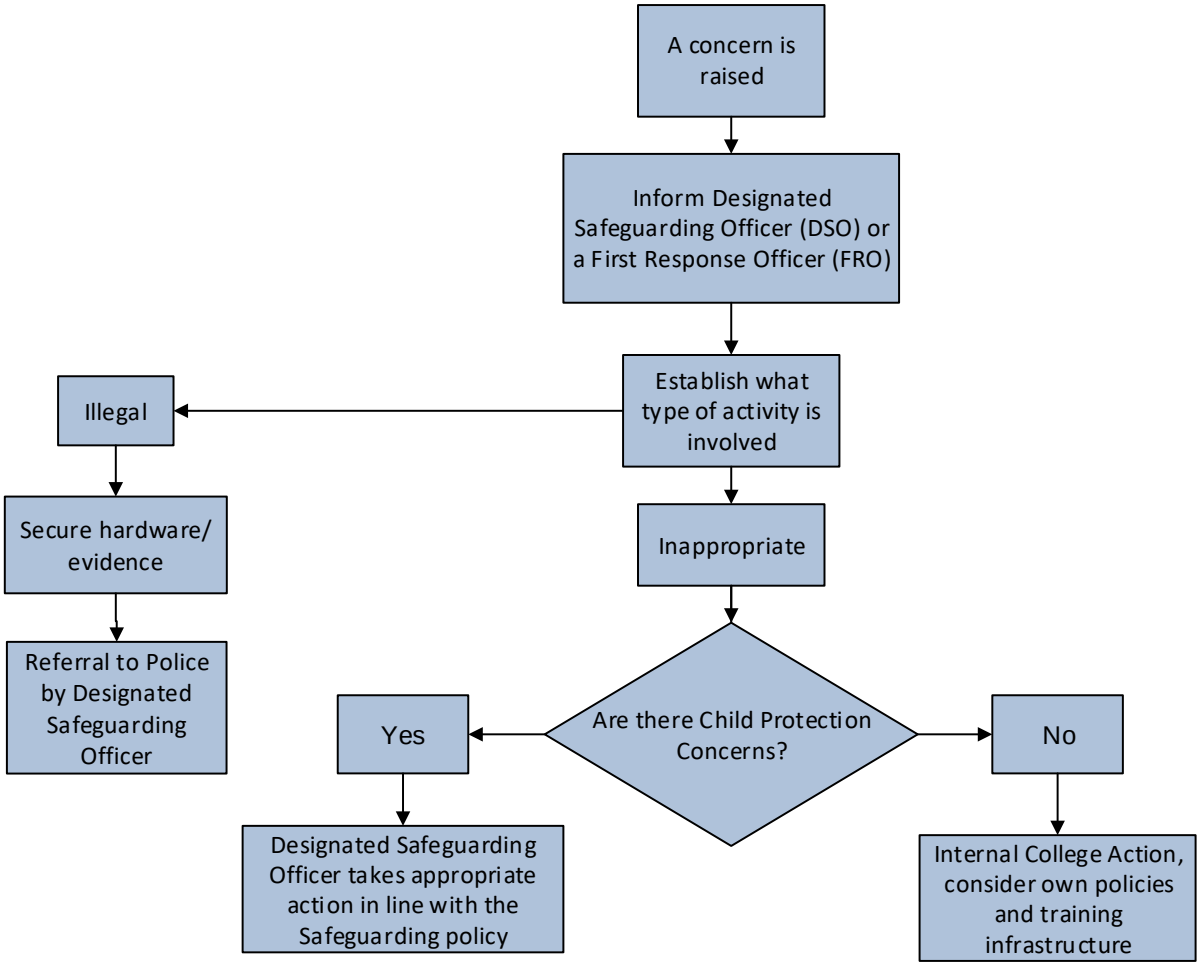
Digital You! – Weston College Student Zone
https://weston.sharepoint.com/sites/WC_StudentSharePoint/SitePages/Digital-You!.aspx

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/

# Appendix 1 – Incident Management Process



# Appendix 2 – 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 are 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 for teaching, learning and assessment requires further understanding of 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 use the College's Canvas VLE known as 'TIDE' 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.

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/)