E Safety Policy

Updated:
Jan 2015
June 2016
Jan 2018

Policy Version Number:	3	
This policy applies to :	All students and staff.	
Related Documents/ Policies:	Safeguarding policy, Equality and Diversity policy, Acceptable use policy, Information security code of practice, Email and internet policy.	
Author:	Emma Hart	
Area:	Safeguarding and IT use.	
Date of latest review:	January 2018.	
Changes made/Reason for Review:	Regular review.	
Trust/LGB/Committee Approval required?	LGB approved and SLT approved.	
Approved by/Date:	SLT	January 2018.
Date of Next Review:	January 2019.	
Equality Impact Assessment	In place.	
Linked to College Value:	Well-being and safety of all. Link to Family value: 'positive aspirations of a free and happy future'.	

Introduction

Oldham Sixth Form College recognises the benefits and opportunities which 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 variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. The term 'e-safety' is used to encompass the safe use of online technologies in order to protect students and staff from known and potential risks. In furtherance of our duty to safeguard students, we will do all that we can to make sure our students and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant college policies e.g. Safeguarding, IT related policies, Anti-Bullying and HR policies.

Policy Scope

The policy applies to all members of the College community who have access to the college IT systems, both on the premises and remotely. Any user of College IT systems must adhere to the E-safety Policy and Acceptable Use Policy. The e-safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones (inc. 'smart' phones), social networking sites, e.g. Facebook, Twitter, Instagram etc.

Roles and Responsibilities

There are clear lines of responsibility for e-safety within the College. The first point of contact should be Emma Hart, the Designated Lead for Safeguarding. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All staff are required to complete the online e-Safety training module, and to read through and adhere to this e-safety policy and associated policies. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All students must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their Progress/personal Tutor or the safeguarding/additional support team. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Specific training on this will be undertaken by all staff. Where it is considered appropriate, the safeguarding team will involve additional support from external agencies.
Specific roles and responsibilities:

Designated Safeguarding Lead:

The Safeguarding Lead is responsible for ensuring staff development and training is provided on e-safety, recording incidents, reporting any

developments and incidents to the relevant bodies and liaising with the local authority and external agencies to promote e-safety within the College community.

Students:

Students are responsible for using the College IT systems and mobile devices in accordance with the e-safety policy. Students are expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the College community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies. Guidance is given through tutorial on appropriate internet use, particularly around social media, their digital footprint and the dangers of grooming. Work on cyberbullying is also done in tutorial and College displays reflect this.
E-safety is also the focus of an assembly to all Year 12 students delivered by the Local Designated Officer for safeguarding.

Staff:

All staff are responsible for using the College IT systems and mobile devices in accordance with the e-safety policy, which they must actively promote through embedded good practice. Staff are responsible for completing online staff training on e-safety and displaying a model example to students at all times. See also 'Safer Use of Electronic Media – Guidance for Staff' (Appendix 1).

All digital communications with students must be carried out in a professional manner and contain appropriate content at all times. All staff should apply the relevant College policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the safeguarding team and/or line manager without delay.

E-safe:

The College subscribes to an external monitoring system called E-safe. Reports are generated on concerning staff or student use of computers and/or the internet. These are followed up by the Designated Lead and safeguarding team, as well as key pastoral staff. In the case of staff concerns, the principal and Director of MIS and HR are consulted and appropriate discussion and follow up takes place. All findings are recorded and trends are identified.
Where appropriate, liaison takes place with external agencies e.g. the Channel team for Prevent concerns.

Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored in line with the E-mail and Internet Policy.

Behaviour

Oldham Sixth Form College will ensure that all users of technologies adhere to the standards of behaviour as set out in the Acceptable Use Policy. The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and student should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police or other appropriate agency.

Guidance for staff on the 'Safer Use of Electronic Media' is provided in Appendix 1. Guidance for students will be issued at induction and in appropriate lessons/tutorial.

Personal Information

Any processing of personal information needs to be done in compliance with the GDPR (General Data Protection Regulation). Personal information is information about a particular living person. Oldham Sixth Form College collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The College will keep that information safe and secure and will not pass it onto anyone else without the express permission of the student or parent/carer.

Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

For students

Issues associated with e-Safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate, when making use of the internet and technologies in class.
Students 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. The Acceptable Use Policy is displayed and must be agreed to whenever students log on to the college network. Within classes, students 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 be asked to complete the online e-safety module as part of their induction to the College. Further e-safety training will be delivered to all or staff or groups of staff as appropriate. The Acceptable Use Policy is displayed and must be agreed to whenever staff log on to the College network.

Incidents and Response

Where an e-safety incident is reported to the College, this matter will be dealt with very seriously. The College will act immediately to prevent, as far as is reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their Progress/Personal Tutor or to the college Designated Safeguarding Lead. Where a member of staff wishes to report an incident, they must contact their line manager or the DSL. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Appendix 1

Safer Use of Electronic Media – Guidance for Staff

Introduction

1.1 Oldham Sixth Form College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement, and staff should feel that they can use electronic media such as social networking sites to communicate with others. It is essential, however, that you take care with the information you make public and remember that once a comment or posting is made, it may not be possible to take it back; there will always be a permanent digital record of it.

1.2 As a College employee, you should remember your public role and always consider how your conduct could affect your professional reputation and the reputation of Oldham Sixth Form College.

1.3 This guidance is intended to give you a number of simple hints to assist you to keep your information safe when using electronic media and to protect you from putting yourself and your employment at risk.

What is a Social Network Service?

2.1 Social networking encourages communication and the sharing of information. Social networking websites are used regularly by millions of people and focus on building online communities of people who share interests and/or activities or who are interested in exploring the interests and activities of others.

2.2 Currently the most popular social networking sites are Facebook, Twitter and Instagram:

Using Facebook, Instagram and Linkedin

3.1 In order to stay safe, you should:

- Create separate ‘professional’ and ‘personal’ profiles and use them accordingly. Keep your professional and personal life separate – it is recommended that you don't become ‘friends' with any of your current or former students on your personal social networking site. Remember your role as a member of College staff and that you should always consider how your conduct could affect your professional reputation and the reputation of the college;
- Set your social networking profile to private so that only your chosen friends can see any photos you publish on it;
- Think before you post any photos of yourself (or comments) on the Internet - ask yourself if you would be comfortable with others such as your colleagues, manager, students, their parents, etc seeing them;
- Make sure that you use a strong password with a combination of numbers and letters and that you keep this password safe. If you use a public or shared computer to access you social networking site (outside of college), cancel any auto-login or ‘remember me’ functions and always make sure you log out at the end of the session. This will prevent anyone from accessing your account.

Using Twitter

4.1 Twitter is a free social networking and micro-blogging service that enables users to send and read messages known as *tweets*. Tweets are text-based posts of up to 280 characters displayed on the author's profile page and delivered to the author's subscribers who are known as *followers*. Senders can restrict delivery to those in their circle of friends or, by default, allow open access. Users can send and receive tweets via the Twitter website, Short Message Service (SMS) or external applications.

4.2 In order to stay safe when using Twitter, you should:

- Check who is following you. This will enable you to block anyone you do not wish to see your "tweets” (updates). Once you've logged in, Twitter shows your home page. Click on "followers” in the upper right-hand menu. There you'll see a list of everyone who has subscribed to be updated whenever you post something. You have three options for each follower: You can click their picture to see their own Twitter page; you can choose to follow them as well; or you can block them from seeing your updates or "tweets”. You may want to block colleagues and students, etc from seeing your updates if you are posting personal items.
- Set your privacy settings: Again, this will limit who sees your updates and also enable you to change your user name so it is not your actual name. In the top right sidebar menu on Twitter there is an item called "settings.” Go here to control what others can find out about you.
- Pick a user name that's not your actual name: Your user name is also the URL that Twitter gives you and the name all your tweets are posted under. To separate your work life from your home life, choose something that affords you some degree of anonymity on Twitter but also remember to choose something appropriate. You could create two separate accounts one for professional use and the other for personal allowing this separation to take place.
- Your profile picture: If you don't want colleagues or students to follow you on Twitter, you might not want to put up your own photo. Consider using a graphic or some sort of icon. If you do want to be recognised, consider not posting anything that shows you in a way that you wouldn't want to appear if you were actually standing in the classroom.
- Don't talk about work in your "One Line Bio”: Twitter offers a one-line biography of up to 160 characters with which to describe yourself. Consider mentioning your hobbies or other interests instead of your job title or where you work.

How do I get offensive content taken down?

5.1 If upsetting or inappropriate images or information is found on the Internet the first person to

contact is the person who is responsible for posting the material. If this is not possible then you can contact the service providers and request the information to be removed.

5.2 The following contact details will help you in the event that you discover any comments or postings which you consider to be offensive:

- FACEBOOK – Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to abuse@facebook.com or www.facebook.com/safety
- TWITTER – To report violations of privacy or threatening behaviour guidelines are published on http://help.twitter.com/forums/26257/entries
- INSTAGRAM – Reports can be made by clicking on **Report Inappropriate** and following the link for spam, scam or abusive content.
- YouTube – Logged in YouTube members can report inappropriate content by using the 'flag content as inappropriate' function which appears under every video. http://icanhaz.com/YouTubeSafety.com