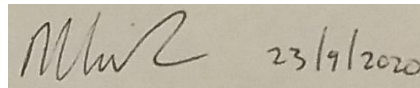**CYNGOR SIR *POWYS* COUNTY COUNCIL**

Ysgol Pontrobert

Use of Social Media and E-safety Policy for staff working in schools

This document applies to all staff working in schools with the exception of staff directly employed by Powys County Council, centrally employed teaching staff or staff such as inclusion services staff. Such staff are subject to the Council's Social Media Policy.
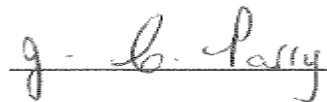
It is highly recommended that schools adopting this policy require any contractors working in the school to abide by the policy.

Cadarnhawyd gan y Corff Llywodraethol **/ Policy approved by Governing Body**

Llofnod Cadeirydd / **Chair's signature:**

Llofnod Pennaeth / **Headteacher's signature:**

Awst / August 2020

Dyddiad adolygu **/Review date:** Awst / August 2021

E-Safety notes

This Policy is a valuable addition to the collection of policies that make up the school approach to online-Safety using the 360 Degree Framework as it adds specific references to Powys Corporate policies and general guidance which reinforces current guidance and policy statements.

In terms of inclusion into the 360 Degree Framework, schools may wish to add it as a separate Appendix and make reference to it within their existing Social Media Policy document. This new policy and the amended Social Media Policy can then be ratified at the next meeting of the Governing Body.

However, attention is drawn to Section 5.4 which appears to indicate terms on which a personal device can be used to take images of pupils. Schools are, of course, free to decide on these issues but it is suggested that a simple ban on this practice is more prudent and easier to implement.

Revisit your 360safeCymru Online Safety Review

Contents

Appendices:

Use of Social Media and E-safety Policy for staff working in schools, Version 1 2017

POLICY HISTORY – VERSION 1, 2017

1   Policy statement

1.1   This policy sets out this School's policy on social media and e-safety issues both inside and outside work. The objectives of this policy are to:

- Set out the key principles and code of conduct expected of staff in this school in respect of use of social media and e-safety so that pupils and staff are safeguarded.

- Ensure that social media is used in a way that treats colleagues and members of this school community with professionalism and respect.

- Ensure that everyone at this school is protected from any malicious cyber bullying and misinterpretations which can arise from the unsafe use of social media.

- Ensure that staff and the whole school community know where to access further information about e-safety.

- Ensure that that staff feel able to report any concerns about breaches of e-safety to a nominated person for e-safety (where this is not their line manager or head teacher.)

- Ensure that staff understand their responsibility to also protect themselves and the reputation of the school by using social networking sites responsibly outside work.

1.2   School staff have a responsibility to safeguard the welfare and best interests of pupils as well as to maintain public confidence in their integrity. It is therefore expected that they will adopt high standards of personal conduct both in and outside school in order to maintain the confidence and respect of their colleagues, pupils, and public in general and all those in the whole school community.

1.3   A guide to roles and responsibilities is contained at **Appendix A**

1.4   Safe practice also involves using judgement and integrity about behaviours in places other than the work setting. School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

1.5   The guidance contained in this policy identifies the behaviours that are expected of schools' staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct, may bring into question their suitability to work with children and young people, which may result in disciplinary action being taken against them.

1.6   It is important that staff and others to whom this policy applies are fully aware of their responsibilities and are educated regarding its implications in order to raise awareness.

1.7   In ratifying this policy the Governing Body is also approving the Code of Conduct for School Staff in Relation to e-Safety contained at **Appendix B**.

2   Purpose and scope

2.1   This policy sets out [Name] School's (the School's) policy regarding the use of social media for both work-related and personal purposes. It applies to all staff employed by the School.

2.2   Used correctly, social media is a powerful tool helping to connect the School with citizens. It is a key communications tool and highlights our commitment to openness and transparency.

2.3 This policy provides a framework to help the School and staff to protect pupils and to avoid potential problems, including the risk of disciplinary action, damage to the School's reputation and/or legal action being taken against the School.

2.4 This policy will apply to all teaching and non-teaching staff employed in Powys schools. This policy also applies to governors, friends and volunteers working in Powys schools. It is not intended to apply directly to pupils or parents for whom advice on online or e-safety for parents is available on a variety of reputable websites including the NSPCC and kidscape.

2.5 This policy takes account of employment legislation and best practice guidelines in relation to e-safety in addition to the legal obligations of governing bodies and the relevant legislation. This includes:

  • Data Protection Act 1998
  • Computer Misuse Act 1990
  • Copyright, Designs and Patents Act 1988
  • Freedom of information Act 200
  • Human Rights Act 1998
  • Regulation of Investigatory Powers Act 2000

2.6 Other relevant legislation may, during the life of this policy, become enacted and will apply when pertinent.

3 Safeguarding pupils

3.1 Current school safeguarding policies apply to any activity on social media and should be adhered to at all times. However, where an employee will be using social media in a way that will potentially give access to the personal information of under 18's or vulnerable adults, the staff member concerned must be DBS checked. No employee may access any information pertaining to a vulnerable adult to minor under the age of 18, unless expressly required to do so as part of their role; where a staff member is in any doubt, they should discuss any concerns or queries with their line manager.

3.2 The school has adopted a code of conduct for e-safety which sets out the standards of behaviour and conduct required from staff in respect of electronic communication. This code is set out at **Appendix B**. In instances where there has been a breach of this Code of Conduct, the following will apply:

3.3 Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the School's Disciplinary Procedure and it is possible that this may be considered to constitute Gross Misconduct and could therefore lead to dismissal.

3.4 The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

3.5 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Head teacher of the justification for any such action already taken or proposed. The Head teacher will in turn seek HR advice where appropriate.

4   Using School equipment for personal use of social media

4.1   Procedures for the use of the internet by employees carrying out work on behalf of the School and/or using School-owned equipment and facilities is governed by Powys County Council's Internet Acceptable Use Policy, Version 6. Employees are reminded that this guidance states:

"At the discretion of your line manager, and provided it does not interfere with your work, the Council permits personal use of the internet in your own time (for example during your lunch-break).

All personal usage using School provided equipment must be in accordance with this policy. Your computer and any data held on it are the property of Powys County Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory, and internal policy requirements."

5   Use of personal mobile devices at work

5.1   School staff should be aware of the example they set pupils in the use of mobile devices and should not use personal devices or use school equipment for personal matters during pupil facing working time.

5.2   If an employee is deemed to be spending excessive time attending to personal matters during working hours, it is possible for this to be classed as misconduct/ gross misconduct under the School's Disciplinary Policy. Excessive use of personal mobile phones and other devices during working hours for phone calls, text messaging, internet browsing or social networking is therefore not permitted.

5.3   Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

5.4   Staff should exercise extreme caution in photographing pupils and, without exception, this must be for professional purposes only. This is limited to photography used to improve teaching or pupil performance (e.g. filming a drama performance for feedback) or which celebrate academic or sporting achievement. Any such photographs must be downloaded to an appropriate, secure school device and deleted from the staff member's device at the earliest opportunity. It is recommended that this is on the same day, but in any event must be within one week. It is beholden upon the member of staff to ensure the security of their device and this content until any such images are deleted.

6   Personal use of Social Media

6.1   Whilst the School respects the legal rights of all individuals, employees need to be aware that what they do and say outside of work can often compromise their position inside work. It is also important to note that other people's perceptions need to be considered when using social media.

6.2   This policy covers the responsibilities of employees both inside and outside work time in relation to their responsibilities to the School.

6.3 Guidance on personal use of social media is attached at **Appendix C**.

6.4 Additional guidance for registrants of the Education Workforce Council (i.e. Teachers and Teaching Assistants) is attached at **Appendix F**.

7 Using social media for communicating in a professional capacity

7.1 Employees must ensure that they have formal authorisation to use social media on behalf of the School and follow all set protocols. All areas wishing to use social media to communicate with the public must first gain authorisation from their respective Headteacher. Once authorisation is gained, the service should contact Powys County Council's Communication Team to talk through the plans and to gain any advice regarding training and approach.

7.2 Social media is becoming an increasingly powerful tool for schools that should be utilised in teaching and learning. However, e-safety is also the responsibility of all staff in school. It is particularly important therefore that staff are provided with information to increase their understanding of e-safety issues to help prevent any breaches that will ensure that staff and pupils are kept safe in school. This may include for example 'cyber bullying' which takes place when an individual or group of people use technology such as the internet, mobile phones, email, chat rooms or social networking sites to bully, threaten or embarrass their victim.

7.3 Although many pupils, parents and guardians use social media tools; not all do. It is therefore essential to ensure that everything a school communicates on social media is also communicated using other methods. There are times when social media alone can be used to push out last minute information but planned, controllable events must always be communicated using a variety of digital and traditional media.

7.4 Social media is a fast moving medium. Schools need to ensure that any content remains current and is frequently updated and checked for feedback. As a general rule, "status" dialogues should be updated at least twice a week. Messages should be either bilingual on one account or two accounts can be operated (in both Welsh and English) with identical content, in line with Powys County Council's Welsh Language Policy.

7.5 Staff should ensure that they do not breach copyright on any images they upload to social media.

7.6 Information included on social media and must be accessible in accordance with the requirements of the Equalities Act 2010. For further guidelines see the Corporate Design Guide on page 3575 of the Powys staff intranet.

8 Monitor and respond to feedback

8.1 Social media is primarily about two-way communication. Whilst it can be used as a broadcast tool, the nature of social media carries with it the inherent risk associated with feedback / criticism in the public arena.

8.2 It is the school's responsibility to manage its own social media accounts. All feedback (comments, etc.) to the School through social media should be monitored on a daily (weekday) basis. Feedback that requires a response must be acknowledged within one working day (or within 5 working days maximum). Where action is required, bear

in mind that excessive delay will have a negative impact on the School's reputation. Where a staff member does not know the answer they should immediately put a holding statement in place, such as "Thank you for your comments, I'll find out and get back to you as soon as possible". Schools should comment on their own school's business only. If somebody makes a comment off-subject give them contact details for the school or service area involved or contact the communications team for advice.

8.3   Whilst there is a need to remain professional at all times, an informal, conversational tone is the most appropriate for social media channels. Staff using interaction tools (i.e. "wall" comments) to respond to criticism, should ensure they are calm and courteous. Be prepared for a two-way conversation and be aware that people are entitled to their views. Staff must make sure that what they say is factual and avoid unnecessary or unproductive arguments. Schools are advised to use their judgement to manage their accounts on a day to day basis in terms of what is appropriate/legal within the context of free speech. But if lines become blurred and they are unsure about whether to remove comments, block users etc. then the Communications Team can provide support and advice.

8.4   It is also helpful to advise the Communications Team if a situation is likely to become a wider public relations issue. Being locally managed, schools are able to speak to the press directly. However the council's Communications Team is able to help and advise, particularly on sensitive issues.

9   Handle offensive comments swiftly

It is the school's responsibility to manage any social media accounts and to monitor offensive content. If it becomes necessary to remove offensive, defamatory or libellous comments from other users, the school may wish to consult the Communications Team, and inform users via a statement such as: "This comment was removed because moderators found the content offensive. I will respond to your comments but please respect the views of everybody who comes here."

10   Related Policies
Use of Internet/ Acceptable Use Policy Version 6
Data Protection Policy
Disciplinary Policy
Fairness and Dignity at Work Policy
Grievance Policy
Official Code of Conduct
Complaints Policy
Equality Policy
Safeguarding Policy
        And any other relevant policy that may be added during the life of this policy.

11   Abuse of the Guidance

The School will take seriously any occasions where social media is used inappropriately. Any complaints of this nature will be considered in accordance with the School's Disciplinary and Grievance Policies.

Further advice and guidance on this policy can be gained from the Powys County Council Communications or Human Resources Teams. Links to resources and useful websites are contained at **Appendix E**

Use of Social Media and E-safety Policy for staff working in schools, Version 1 2017

APPENDIX A
ROLES AND RESPONSIBILITIES

The Governing Body will ensure that:

- The school recognises its legal responsibility to protect staff from unlawful harassment as well as mental and physical injury at work.

- The school's Social Media and E- Safety Policy (and related polices and practice such as staff induction) will be reviewed and monitored periodically so that staff, pupils and parents feel confident

- The school effectively supports e-safety.

The Head teacher will ensure that:

- The whole school community including staff, pupils and parents are signposted to information, policies and practice about e-safety.

- Staff are provided with information and professional development opportunities with regards to understanding, preventing and responding to cyber bullying.

- Where it is not the line manager or Head teacher, ensure that the school has a nominated person as an e-safety lead to oversee, manage the recording, investigation and resolution of cyber bullying incidents.

- Staff are clear about to whom who they report any breaches of e-safety.

The nominated person as the E-safety lead will ensure that:

- Staff receive appropriate support to deal with and or respond to claims of cyber bullying or any other breaches of e-safety.

- Incidents are dealt with in a timely manner.

- Where appropriate and in agreement of the wishes of the person who has reported the incident, report the actions to the police.

- Powys County Council is contacted as appropriate.

Staff should ensure that:

- They familiarise themselves with this e-safety policy and related procedures

- They understand and adhere to the schools E-Safety Code of Conduct (see Appendix B)

- They never personally commit, contribute to or conspire towards cyber bullying.

- They use social networking sites in an appropriate manner including editing or deleting any historical materials.

- They immediately report any incidents that they become aware of, whether past or current, to the nominated person and seek support.

- They keep any records of the abuse including text, e-mails, voice mails, website or instant message.

- Screen print messages are made or web pages and times, dates and addressed of the site are noted.

APPENDIX B: CODE OF CONDUCT FOR THE SCHOOL'S STAFF IN RELATION TO E-SAFETY

The School's staff must:

- Communicate with pupils and staff in an open and transparent way using the school phone number and email address. (Personal e-mail addresses should never be given to pupils or parents.)

- Keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents in a professional capacity. (There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle, or where staff are transport escorts or where for PTA purposes for example both staff and parents have exchanged personal numbers). Similarly there are specific occasions where, as an exception, it is appropriate for staff to share details with parents, for example emergency contact details during school trips. These contacts/occasions however, will be easily recognised and openly acknowledged. In any other situation, or where a staff member is in doubt, such sharing must be sanctioned by the headteacher. Staff have a responsibility to make sure that any such contact is known to the senior leadership team.

- Keep their mobile phone secure whilst on school premises. All mobile phones should be switched off or silent whilst staff are on duty unless there are good reasons that have been confirmed with a member of the senior leadership team.

- Never 'friend' or otherwise connect with a pupil at the school where they are working onto their social networking site. There may be exceptions e.g. where a teacher's own children attend the school. All staff are expected to exercise professional caution and staff registered with the Education Workforce Council are required to comply with the Council's Code of Professional Conduct and Practice.

- Never use or access social networking sites of pupils and should never accept an invitation to 'friend' or otherwise connect with a pupil other than where the exceptions above apply.

- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings (this should include past postings.)

- Be aware of the potential of on-line identity fraud and to be cautious when giving out personal information about them which may compromise their own personal safety and security.

- Never share their work log-ins or passwords with other people.

- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

  The following are not considered acceptable at this school:

- Under no circumstances should staff make highly derogatory defamatory, rude, threatening or inappropriate reference to any staff member, governor, pupil, parent or school activity/event during their social use of the internet or other communication media. Positive or neutral references to individuals should only be made with that person's permission.

- The use of the school's name, logo, or any other published material without written prior permission from the Head teacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

Personal information on social networking sites:

- Some social networking sites and other web-based sites have fields in the user profile for job title etc. School staff should carefully consider the information they input on the site as it may identify their profession or the school where they work. In some circumstances this could damage the reputation of the school, the profession or the local authority.

- In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

- All staff should regularly review their social networking sites and privacy settings to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published more widely.

- Employees need to ensure that when they are communicating about others, even outside work, that they give due regard to the potential for defamation of character.

- Personal accounts must not be used as a school communications channel.

Maintain confidentiality

- Staff should never publish or disclose any information about the School or Powys County Council which is not already in the public arena. A breach of confidentiality could result in disciplinary and / or legal action being taken against the employee.

- Staff should not publish or report on conversations that are private or internal to the School or Powys County Council. Nor should they cite or reference the School or sections of it, pupils, parents, employees, managers, partners or suppliers.

- Be mindful that whatever is published may be in the public arena for a long time and that doing so may result in disciplinary action being taken.

Retain professional integrity

- Staff should ensure that their online activities do not interfere with their job, colleagues or commitments to pupils, their parents and the public. Online activities must always adhere to the staff Code of Conduct.

- Relationships with pupils, parents, the public etc. should always be kept professional and respectful. The School acknowledges that in smaller communities, the lines can become blurred particularly, for example where a parent is also a friend or acquaintance – in such cases, employees should disclose an interest to their line manager - common sense and discretion should be applied and all employees are specifically required to make themselves aware

of the provisions of the Code of Conduct in this regard. In all cases, clarity should be sought from the employee's line manager.

- Social media is increasingly used as a combined professional and personal space, where they might share personal anecdotes and professional views. Social media sites such as LinkedIn and Twitter, are good examples of online spaces where this is common practice. The School is supportive of this approach in principle, but staff must be vigilant to ensure that where they identify themselves as an employee of the School, content should never be highly political (in relation to the School or Powys County Council) and free of any highly derogatory comment that may bring the School or Powys County Council into disrepute.

- When using social media tools to interact with colleagues in a professional capacity – for example with Yammer – do not treat the tool as a confidential space for confidential or personal conversations. Always assume that anything shared on such tools are in the public domain

- Registrants of the Education Workforce Council (i.e. Teachers and Teaching Assistants) should also refer to the Council's 'good practice guide' for registrants attached at Appendix F

Be respectful to colleagues

- Using social media to attack or abuse colleagues (harassment and "cyber" bullying) will be regarded as gross misconduct and will not be tolerated by the School.

- Staff are expected to respect the privacy, feelings, reputation, and position of others they work with.

- Individual staff should not be named or quoted on social media without their prior consent

- Images of colleagues should not be published unless consent has been given

- Staff must not upload or tag colleagues in posts which are defamatory, offensive or sensitive. Complaints of this nature will be dealt with under the School's policies, e.g. Disciplinary, and Grievance.

The School's reputation

- The School acknowledges that many staff are also local residents. However, regardless of where they live, employees must not make derogatory comments about the School or Powys County Council as this can be damaging to the School's, or Powys County Council's, reputation and to an individual's professional reputation. Such activities may also contravene a school's commitment to safeguarding children.

- Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Powys County Council could result in formal action being taken. This includes the uploading of photographs which might put the school into disrepute.

- For the school's protection as well as the staff member's, it is important that employees stay within the legal framework and are aware that libel, defamation, copyright, and data protection laws apply.

Political statements, or the promotion of political parties

- When using social media in a professional capacity employees must not:
  - ✕ Make political statements, comment, share or get involved in political arguments;

    and/or
  - ✕ Make their own views about School or Powys County Council policy / services known
- Where staff are candidates in a local, general, Welsh Government or European elections, police commissioner elections or any other public office position, then they must inform the Solicitor to Powys County Council so that an exemption for political content can be made, but in such circumstances, candidates must not seek to use their status as an employee as an endorsement of their character or politics.
- Staff should speak to a member of the Communications team before making any public comments.

APPENDIX D
GLOSSARY OF TERMS

Definition of terms

1) Disrepute – loss or want of reputation; discredit or being held in low esteem. Examples are:

John's Facebook profile stated that he worked for [Name] School and in a wall post on 24th June he stated that he worked with a bunch of monkeys who were deliberately wasting public money on stupid schemes that would never produce what they promise.

or

A video posted on the School's Facebook page showed staff seeing who could be fastest to complete an obstacle course on the school playing field whilst holding pints of beer.

2) Excessive use - If something is described as the amount or level of something being excessive, this means it is deemed to be disapproved of; because it is more or higher than is necessary or reasonable.   "Excessive use" would be judged by managers based on the impact it has on the quality and quantity of work produced and the impact on colleagues.

3) Exceptional Circumstances - Exceptional situations and incidents are unusual and only likely to happen very infrequently. With regard to this policy "exceptional circumstances" would be considered by managers based on this definition. An example could be if an employee has an ill older relative or child and needs to keep in touch with other relatives.

Resources:

The Welsh Government has produced a set of resources aimed primarily at teachers in schools to support the teaching of safe and responsible use of the internet as well as other e-Safety issues: **http://hwb.wales.gov.uk/esafety-resources**

Safer Internet Day is celebrated globally in February each year to promote the safe and positive use of digital technology for children and young people. Further information is available on the following link: **www.saferinternet.org.uk/safer-internet-day**

Internet safety websites:

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

https://www.kidscape.org.uk/advice/cyber-bullying/

https://www.internetmatters.org/schools/

www.childnet.com

https://www.thinkuknow.co.uk/Teachers/

https://360safe.org.uk/

http://www.teachingideas.co.uk/themes/staying-safe-online

Trades unions and associations also have useful guidance and training.

Education Workforce Council

Guide to using social media responsibly

February 2016

1.0 Introduction

Social media are a range of web-based applications that allow people to create and exchange content. The popularity of social media has grown rapidly in recent years with widespread use of sites such as Facebook, Twitter, Instagram, YouTube and LinkedIn, as well as dating websites, blogs, emails, texting and instant messaging.

When used responsibly and appropriately, social media can offer you several benefits as an education practitioner, such as:

- building and maintaining professional relationships;

- giving you access to support networks, providing a means of discussing professional issues and sharing good practice;

- providing access to professional learning opportunities and / or educational resources.

However, there are also a number of dangers and pitfalls you need to be aware of when using social media. This guide aims to help you by highlighting how those dangers and pitfalls could affect you, and potentially your ability to continue practising.

All Education Workforce Council (EWC) registered practitioners are subject to the Code of Professional Conduct and Practice which sets out the key principles of good conduct and practice for registrants. This guidance should be read in conjunction with the Code which can be downloaded from our website.

2.0 Dangers and pitfalls of using social media

2.1 Common issues facing professionals

The way you use social media in your private life is a matter for your own personal judgment. However, you should still exercise caution in the content you upload to any social media site and consider whether it could compromise public confidence in the education workforce.

Using social media can blur the boundary between your private and professional life and these days all professions are subject to far greater public scrutiny making practitioners vulnerable to unintended misuse. It is inevitable that people (learners, parents, public, prospective employers) will be curious about individual practitioners and may try to find out information about you.

It is therefore important you are cautious about which social media you use, and how and with whom you communicate.

Bear in mind:

- the standards expected of you do not change because you are communicating through social media;

- email, texting, blogging and other social media communication encourages casual dialogue. Innocent comments or posts can be misconstrued or manipulated. The 'feel' can be different;

- you can be vulnerable to unintended misuses;

- acknowledging, liking or sharing someone else's post can imply you endorse or support their point of view;

- you can be mentioned / identifiable in inappropriate posts, sometimes without your knowledge or consent;

- your conduct online does not have to relate to learners in order for it to have a bearing on your fitness to practise;

- postings online are subject to the same laws of copyright and defamation as written / verbal communication;

- unwise behaviour online can result in criminal or civil action.

2.2 Privacy and confidentiality

Bear in mind the personal material you might intend only to share with friends or family could be accessible to a much wider audience, and that once uploaded to the web, it may not be possible to delete it or control how widely it is shared.

Some social media sites have privacy settings which allow users to control and put restrictions on who has access to their personal information, but the default settings on some sites may allow content to be shared beyond an individual's preferred, closed network of friends or family. It is therefore important you familiarise yourself with the privacy provisions of any social media site you use, and bear in mind the limitations of keeping information private online.

If you are unsure whether or not communication you post online could compromise your professionalism or reputation, think carefully about the appropriateness of posting it.

In particular, you should be aware that:

- your personal information can easily be accessed by others. Social media sites cannot guarantee privacy regardless of what settings are in place;

- once information is published online, your control of it is lost. It can be difficult to remove as other users may share or comment on it;

- information uploaded anonymously can, in many cases, be traced back to its point of origin;

- information about your location may be embedded within photographs and other content, and available for others to see;

- although individual pieces of information may not breach confidentiality on their own, the sum of published information online can be enough to identify a learner or parent and consequently have potential for reputational damage to you, and possibly your employer.

3.0 Examples of cases investigated by the EWC

The examples below are some of the cases referred to the EWC for investigation relating to social media. These are illustrations of where practitioners have breached the Code of Professional Conduct and Practice:

- a teacher engaged in a sexual relationship with a learner which began with communication via mobile telephone and text messages with sexual content;

- a teacher sent a string of sexually explicit messages via Facebook and Skype to a learner;

- a teacher's computer was found with hundreds of downloaded indecent images on it;

- a teacher with a number of learners as 'friends' on Facebook posted inappropriate comments about drinking and parties;

- a teacher subject to an EWC hearing received disproportionate press coverage when inappropriate photographs and video clips previously posted online were accessed by the press;

- a teacher used an eBay account to illegally sell counterfeit goods;

- a teacher re-tweeted insulting comments about the victim of a serious criminal offence;

- a teacher posed online as a pupil and made a false report to a charity helpline about a senior member of staff.

4.0 Guidance to help practitioners minimise risk when using social media. You should:

4.1 Follow the guidance

- adhere to employer or agency policies, procedures and guidelines using official channels of communication;

- adhere to the EWC Code of Professional Conduct and Practice;

- use trade union and other guidance;

- understand any social media application before using it, and be clear about its advantages / disadvantages.

4.2 Act responsibly

- conduct yourself online in a way which does not call into question your position as a professional;

- consider your online persona and how others perceive you. Be careful when writing profiles or establishing email addresses;

- never create a false identity;

- consider who or what you associate with online, and always maintain professional boundaries with learners;

- never exchange private phone numbers, personal e-mail addresses or photographs of a personal nature with learners;

- never accept or initiate Facebook friend requests, or other such invites, with current or former learners. Discretion should be used when dealing with friend requests from parents;

- ensure your privacy settings are appropriate, and be aware that not all information can be protected on the web - there is no privacy mechanism that is 100% guaranteed;

- ensure your settings prohibit others from tagging you in any photograph or update without your permission;

- be aware of photographs published online which include you, and where they may be posted;

- do not discuss learners, parents, or colleagues online, or criticise your employer;

- protect yourself by always logging out of any social media site you are using at the end of a session.

4.3 Not be complacent

- be aware that others may try and view your online social media profiles, or even just Google your name. For example, potential employers, learners, parents, press officers;

- appreciate that learners will be curious about you, and may search the internet for your personal information;

- manage your privacy settings, especially in relation to photos. If you do not, assume the information you post will remain in the public domain, and be capable of being accessed, changed, shared and manipulated;

- audit and re-evaluate information about your online self regularly, and ask others to remove any undesirable content about you;

- use strong passwords and change them regularly. Never share passwords;

- protect your mobile telephone, laptop and/or tablet. Know where they are and who has access to them;

- bring any social media concerns to the attention of your employer or agent as soon as you become aware.

4.4 Summary

Before posting anything online, ask yourself:

- might what I'm posting reflect poorly on me, my employer or profession?

- is my intention to make the post driven by personal or professional reasons?

- am I confident that the posting, if accessed by others (colleagues, public, parents etc.) would be considered reasonable and appropriate for a professional?

5.0 How we can help you further

- The EWC offer presentations which focus on fitness to practise and the use of social media. If you or your employer would like to arrange one in your school or college please contact (information@ewc.wales);

- The EWC's Code of Professional Conduct and Practice for Registrants with the Education Workforce Council, and Information about the EWC's fitness to practise work can be found on its website www.ewc.wales/site/index.php/en/fitness-to-practiseFitness

- Any queries should be referred to the Fitness to Practise Team at fitnesstopractise@ewc.wales