Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Education Safeguarding Team, Kent County Council
August 2017

Protecting Professionals Online: Considerations for Leaders, Managers and Designated Safeguarding Leads

All staff should know what their educational setting believes to be safe and appropriate online behaviour.

Leaders, managers and Designated Safeguarding leads (DSLs) should ensure that all staff:

- Read the Acceptable Use Policy (AUP) and online safety policy.
- Are familiarised with policies and procedures regarding safe technology use and classroom practice.
- Understand and follow the procedures for reporting and recording online safety incidents or disclosures.
- Access quality and up-to-date online safety training on a regular basis.

Leaders, managers and DSLs should ensure that all staff:

- Are aware that civil, legal or disciplinary action can be taken against staff if they are found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in professional abilities.
- Are aware of the policy regarding staff contact outside of work with children and parents/carers:
    - Do not use or give out personal contact details to children or parents/carers, for example email addresses or mobile numbers.
    - Ensure that all communication with learners, parents and colleagues is professional and via official school/setting communications such as work provided emails/numbers to protect both staff and pupils. Communication should always be transparent and open to scrutiny.
    - Understand that it is recommended that staff do not accept friend requests or communications from learners or their family members (past or present).
    - If there is a pre-existing relationship then this should be discussed with the DSL and/or a member of the management or leadership team.

Leaders, managers and DSLs should encourage all staff to consider:

- Their personal use of the internet carefully, but not banning them from doing so.
- The need to understand and manage their digital reputation, including the appropriateness of information and content that they post online.
- The need to discuss online expectations and behaviour with friends and colleagues.
- The need to make sure any social networking sites they use are set to private, and that they check their settings frequently.
- That no matter what privacy settings are used, they are aware that anything posted online can become public and permanent, can be misinterpreted and/or used without their knowledge or consent.

DSLs should ensure that all members of staff are aware of how to report concerns:

- If they or another member of staff is affected by cyberbullying, they should inform the Headteacher/line manager and follow guidance to report the abuse given by the website (if appropriate).
- All staff should be made aware of the internal and external reporting mechanism regarding online safety concerns.
- All staff should be made aware of the whistleblowing policy.