

**CAEDMON COLLEGE WHITBY POLICY DOCUMENT
ACCEPTABLE USE – ICT AND E-TECHNOLOGY**

Acceptable Use Agreement – ICT and E-technology

College Governance Status

This policy was introduced in July 2011 following guidance from North Yorkshire County Council and was first adopted by the Governing Body on 14 September 2011. It will be renewed in the light of new Local Authority or Government guidance or every three years.

| Review dates | By Whom | Approval date |
|---------------------|---------------------|----------------------|
| October 2012 | Staff and Governors | 17.10.12 |
| October 2016 | Staff and Governors | 18.10.16 |
| February 2017 | Staff and Governors | 27.03.17 |
| September 2017 | Staff and Governors | 28.09.17 |
| September 2020 | | |

Signed by the Chair:



This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT and the related technologies such as email, the internet and mobile devices. Members of staff should consult with a designated ICT Technician/Manager for further information and clarification.

Members of staff:

- Must only use the College's email, internet and intranet and other related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body. Individual employees' internet and other related technologies are monitored and logged and can be made available, on request, to line managers.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Should not use school information systems or resources (eg, cameras, laptops, tablets memory devices) for personal purposes without specific permission from the Principal; they should only be used for professional purposes.
- Are not permitted to use personal portable media for storage of College-related data/images (eg, phones, tablets, USB stick) without the express permission of the Principal.
- Should ensure that personal data (such as data held in CMIS) is kept secure and is used appropriately, whether in College, taken off the College premises, or accessed remotely. Personal data can only be taken out of College when authorised by the Principal or Governing Body and must be encrypted by either hardware or software applications.
- Are permitted to use personal digital equipment, such as mobile phones, tablets and cameras, to record images of students, including when on external trips/visits, with the written consent of parents. These images should be shared with the Marketing/AV team as appropriate and then deleted as soon as possible.
- Should ensure that their use of social networking sites, such as Facebook and Twitter (including external use, as well as during College working hours) does not question or bring their

CAEDMON COLLEGE WHITBY POLICY DOCUMENT
ACCEPTABLE USE – ICT AND E-TECHNOLOGY

professional role, the College or the Local Authority into disrepute. Some examples of recent case law to indicate what is not appropriate are included as Appendix 1 of this policy.

- Are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever. Staff should not assume that because privacy settings are activated on e-technology/social media accounts that these messages/pictures will not be seen by a wider audience that could bring their professional role or the College into disrepute. The cases given in Appendix 1 show how it is possible to breach employment policies and staff codes of conduct through the use of social media outside of working hours. The Governing Body/Principal will investigate any reports of derogatory/potentially damaging comments made using social media, whether made inside or outside of working hours where these could impact upon the reputation/smooth running of the College and/or breach College policy. In such cases, appropriate disciplinary action will be taken as per the College's disciplinary policy. Making defamatory or derogatory comments, or offering threats of violence on social media, has the same legal consequences as writing or saying it to the individual. Legal action can be taken against the person making comments under the Malicious Communications Act 1988.
- Should not communicate with students, in relation to either College or non-College business, via social media sites. College Twitter accounts are not to be used for non-College business.
- Are not permitted to contact or communicate with students, parents or conduct College business using personal email addresses or telephones, without specific permission from the Principal.
- Should not give out their own personal details, such as telephone/mobile number or email address, to students.
- Must ensure that all electronic communication with students and staff is compatible with their professional role, and should be via a central email address – ie, post@ccwhitby.org or that their line manager or other appropriate member(s) of staff, eg the Designated Safeguarding Lead (currently Jonathan Bond) is copied in.

User Signature

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in line with the College's Disciplinary Procedure.

Signature: _____ Date: _____

Name (printed): _____ Post Title: _____

Case law judgements on the use of social media [Source: adapted from Dickinson Dees' handout ref: 20987247; Oct 2012]

- Gosden v Lifeline – Gosden had sent a racist and sexist email chain out of working hours from his home computer to a colleague's home email. His colleague subsequently forwarded it to colleagues at his work place. Gosden's right to privacy was considered. It was decided that he should not have assumed that the email would not go further. Gosden was dismissed. The case went to an employment tribunal and the dismissal was judged to be fair.
- Preece v J D Wetherspoon – Preece had been professional during her working hours about a situation she was unhappy with at work. Later, however, she complained on Facebook about the work situation using abusive comments and mentioned staff names. She said she had thought she had correctly set her privacy settings on Facebook but actually had not. The right to Preece's freedom of expression was considered but the Employment Tribunal considered that her dismissal was fair.
- Two teachers at a primary school allegedly made derogatory comments about people from the area, using Facebook, during the summer holiday. Someone had accessed the Facebook page, printed it and pasted it all over the school gates prior to pupils and staff returning in September. They had also posted copies through local residents' doors. The two staff involved said their comments had been cut and pasted but this did not help their case. It was classed as a criminal case. The two staff resigned.
- Teggart v Tele Techn UK Limited 2011 and Crisp v Apple Retail (UK) Ltd – derogatory comments were made using social media by employees of both firms. Despite the rights to privacy and freedom of expression legislation, the employees posting derogatory comments were judged to be fairly dismissed. The Judge said that privacy settings no longer guaranteed privacy and so this could not be used as a valid excuse.

These cases show how it is possible to breach employment policies and staff codes of conduct through the use of social media outside of working hours. The Governing Body/Principal will investigate any reports of derogatory/potentially damaging comments made using social media, whether made inside or outside of working hours, where these could impact upon the reputation/smooth running of the College and/or breach College policy. In such cases, appropriate disciplinary action will be taken, as per the College's disciplinary policy