# AAT ethics guidance note
# Digital ethics

**Please note** – this document and its contents are for guidance only and do not form part of the AAT *Code of Professional Ethics*. They are designed to provide further information on particular topics of interest that may not be covered in detail within the *Code*. Nonetheless, they do provide insight on best practice and may be used in conjunction with the *Code* when considering matters relating to disciplinary breaches.

## Background

Whenever we talk about change and progress, technology inevitably tends to dominate the conversation. Increasingly the technology is digital and cloud based, raising questions of ownership, privacy and security. In addition, with so much of life lived online, the boundaries of personal and professional are often blurred.

## Why is this an ethical issue?

### Data

As professionals, accountants and finance specialists have always been privy to sensitive information; sensitive both in a business capacity and personally for individuals. Increasingly, that information is moved around digitally – from company to company, across international boundaries and held by the cloud on multiple servers in different jurisdictions.

Just as a client would expect business papers to be held securely in an office, they have the same expectation of their digital information. It is not without good reason that confidentiality plays a major role in the *AAT Code of Professional Ethics*.

As accountants increasingly use cloud accounting platforms for much of their day to day services, questions arise over ownership and access to data when clients disengage services. AAT regularly fields questions in relation to this, as the licensing and access systems of the cloud packages are rarely designed with these issues in mind. Nonetheless, it's clearly a matter of professional ethics that clients should have ready access to their own data.

Data privacy laws are also becoming increasingly strict in support of individual privacy, in part as a reaction to data mining by the tech giants, and it's essential that professional accountants are fully conversant and compliant with those laws. Failure to do so can result in serious professional and financial repercussions.

### Online presence

It's probably fair to say that we're currently in a transition period in relation to online presence, with a shrinking number of professionals with little online presence, and a rapidly increasing number for whom extensive online presence is not only natural, but desirable.

While the marketing and networking benefits of the online world are not in dispute, the proliferation of platforms for individuals to share information and opinions do pose a danger in relation to the

observance of professional ethics and in cases of disclosure of data, potential violation of applicable law.

AAT's *Code of Professional Ethics* requires members to refrain from activity likely to undermine public confidence in the Association or its members and unfortunately, certain online conduct risks breaching that requirement. In the experience of AAT, the vast majority of members currently understand the boundaries and behave accordingly. Nonetheless, we have seen a growth in complaints regarding members using platforms to abuse others based on protected characteristics such as ethnicity, nationality or faith. What is even more worrying is that some of these cases have taken place on ostensibly 'professional' platforms where AAT qualifications and membership are clearly displayed. Responses to these cases have tended to run along defences of 'personal views' or 'retaliation'. Members should be aware that 'retweets' and joining of certain groups may be deemed inappropriate and be mindful of exposing themselves to legal risks. There can be no question that these actions are not defensible when sitting alongside references to the individual's professional standing. Further, it is expected that members observe diversity of views, respect opposing positions and safeguard the dignity of others. Where online critique is made, members should strive to represent evidence-based perspectives.

## What should I do?

**Data**

When considering your personal development explore digital learning to keep up with changes.

Ensure you're secure – five key controls in any compliance framework include technical controls, policy controls, training and awareness, management oversight/organisational visibility and, monitoring and audit.

Cyber Essentials is a simple but effective tool which aims to ensure that the basic level of security is in place. Cyber Essentials compliance can prevent most cyber-attacks and it's also possible to get cyber insurance included with the cost of certification for qualifying organisations.

Know the law – the Information Commissioner's Office (ICO) has various support resources to help on your compliance roadmap. The basics of compliance stem from the data protection principles set out in Article 5 of the *GDPR*. A key aspect of this is the second paragraph which requires that organisations are accountable and able to prove it to others. Recent additions to ICO guidance aim to help with this and include:

An accountability self-assessment which produces a downloadable report to help you determine the next steps. An accountability tracker is also available in Microsoft Excel format.

An SME hub providing various support tools and bite-sized advice.

A self-assessment checklist for small business owners and sole traders to assess how well you comply with data protection law.

Various other self-assessment tools covering direct marketing, CCTV, records management and more.

There is also the European Data Protection Board guidance covering various topics. Whilst the UK are no longer part of Europe our domestic legislation remains to be almost a mirror image of the EU GDPR and so this is still a useful source of guidance and support and remains to be referenced by the ICO.

Understand your systems – understand how any third-party licensing works in terms of data manipulation, storage and transfer in the case of disengagement. This is particularly true if using any kind of 'free' software. As the old adage goes, "if you're not paying for it then you're the product" and the chances are your (and your client's) data is not as secure as it should be.

Be clear with clients – ensure your engagement letters are accurate and current, including any references to third parties (software, platforms, contractors) and up to date privacy policies. Your internal policies should also be clear – in writing and available to, and understood by, all staff.

**Online presence**

Consider all social media activity as you would a professional meeting and behave accordingly.

Ensure that you adhere to your employers' policies.

Ensure the personal and professional domains remain distinct and be cautious that mixing can reduce inhibitions and even innocent actions or statements can be misconstrued e.g. be wary about befriending clients on platforms which are not designed for professional networking (Facebook vs LinkedIn for instance); avoid potentially controversial opinions, or sharing contentious information, on professional sites; avoid using professional designations on 'purely' social media platforms if you wish to use it to air personal views (as opposed to views based on professional opinion). Your profile or 'handle' does not necessarily disguise who you are and social media platforms will hold your registration details.

Remember that you can be identified in just a couple of clicks. Distinguish between your professional and personal contacts in your online networks. For example, you would not be expected to issue a fundraising message to your professional contacts. State on your website and blogs that views expressed are your own and do not necessarily reflect the views of your employer or the Association. Lock the privacy settings on your personal accounts and restrict geolocator tools (that may imply a professional relationship with an organisation, venue or location) and updates. Use photos with caution, ensuring there is nothing offensive or controversial in the background. Restrict people from tagging you.

Consider that a link with a client can imply that you have an association and therefore in of itself breach data that is confidential.

Once information is posted online, you lose control of it. Social media posts can be retrieved many years later, even if you have deleted them. Be sure that your post(s) would not cause issues in later stages of your career and professional life, e.g., potential employers viewing historic content.

Search for your name and credentials regularly and arrange removal of any content that is inaccurate or inappropriate.

Conversations on social media may not be confidential. It is advisable to restrict engagement with clients on a one-to-one basis to email, written or telephone correspondence rather than direct messages on social media platforms. This not only protects the privacy of sensitive data but will also ensure that records and correspondence trails are accurately reflected.

Do not engage with trolls and block individuals who harass, are abusive or trolling. Take screenshots and be prepared that you may need to contact the police where there are two or more related occurrences of harassment.

Posts critiquing a competitor could fall foul of fair competition requirements and this extends to employees and ambassadors of organisations.

Consider carefully all posts and refer to a colleague if you are unsure whether a potential post may infringe upon the AAT requirements. Consider:

- is it factual and not defamatory, harassing, obscene, libellous? Would a direct conversation be more appropriate?
- is it written correctly or could your draft be misunderstood?
- consider copyright, confidential and personal data and acknowledge proprietary information, content or the contribution of colleagues and any other sources.
- do you have full permission to disclose and information or insights?
- could an individual be identified from your post?
- does the post have negative consequences?
- does the post add value?
- is it responsible?
- could the post be perceived as representing the profession, AAT or a collective group? Only those designated by the AAT have authorisation to speak on behalf of the Association.
- does the post represent the values and policy of your organisation or employer? If you are unsure, check first before posting.
- disclose any conflicts of interest or financial incentives.

It's highly advisable to have policies related to social media usage. Policies should be developed through consultation with employees and trade unions if applicable. Policies, the risks with social media and cyber security should be part of inductions and ongoing training, and fully understood by staff members.

## Checklist

1. Get cyber-secure.
2. Ensure policies and client agreements are up to date.
3. Clearly separate the personal and professional online.