

Accredited Registers

Targeted Review – Association of Christians in Counselling and Linked Professions (ACC)

29 September 2023

1. Outcome

The Accreditation Panel (“the Panel”) renewed the accreditation of the Association of Christians in Counselling and Linked Professions ([ACC](#)) following a targeted review focusing on Standard Six.

We found that Standard Six was met.

We issued the following Recommendation:

Recommendation One: The ACC should monitor and evaluate the implementation and integration of the new processes they have introduced to meet the requirements of the Information Commissioner’s Office (ICO) in relation to information security.

2. Background

The Process

We conduct an annual check for each Accredited Register. This is used to monitor whether there have been any significant changes to key processes or significant concerns raised that could affect whether the *Standards for Accredited Registers* (the Standards)¹ continue to be met.

In some cases, where we need further information or where we have concerns, an annual check will be escalated to a targeted review of the Accredited Register. A Targeted Review consists of a more in-depth assessment of specific Standards.

Following a Targeted Review, an Accreditation Panel considers whether the Standard(s) continue to be met. The Accreditation Panel may issue Recommendations or Conditions. In serious cases, it may consider suspending or withdrawing accreditation.

More information about the annual check and targeted review assessment process for existing Accredited Registers is set out in our *Accredited Registers - guidance on renewing accreditation*.²

The Association of Christians in Counselling and Linked Professions (ACC)

¹ [Standards for Accredited Registers 2023 \(professionalstandards.org.uk\)](#)

² [annual-review-process-guide.pdf \(professionalstandards.org.uk\)](#)

The ACC is a UK-wide organisation for the recognition of training in Christian counselling and pastoral care. It registers counsellors and psychotherapists and was first accredited by the Professional Standards Authority in April 2015.

The ACC has a Board of nine trustees and an independent [Register Advisory Panel \(RAP\)](#) 'who hold ACC to account to show that the standards for entry to the Register are upheld. It operates across the four countries of the UK and as of 1 January 2023, there were 899 registrants on the register.

The ACC Annual Check

The annual check involved a:

- review of information provided to the team by the ACC in its annual check form, submitted on 11 May 2023.
- review of 'Share Your Experience' submissions received since the last review.
- check of the ACC's register.
- review of the findings of our previous assessments of the ACC.

During the annual check we became aware of alleged data security breaches and incidents which had been reported to the ICO. Part of the ICO's role is to consider complaints from individuals who believe their data protection rights have been infringed. It does this with the aim of improving the way organisations deal with the personal information they are responsible for.

We initiated a Targeted Review to gain a better understanding of what had happened, and what actions the ACC were taking in response. The Targeted Review focused on Standard Six (Governance), which requires that 'the governance of the organisation supports public protection and promotes transparency, integrity and accountability.' Our minimum requirements³ for Standard Six include that the 'Register should have relevant data processing policies in place, including for holding and processing EDI data.'

3. Assessment against the Standards

Standard Six – Governance

Reasons for Targeted Review

As set out above, we initiated a targeted review in this case was required to gain a better understanding of the incidents reported to the ICO. This involved reviewing the ICO's findings, as set out in its letters to the ACC; and reviewing the actions that the ACC is taking in relation to the ICO's findings.

The Accreditation Panel's findings

³ As set out in our *Evidence Framework*: https://professionalstandards.org.uk/docs/default-source/accredited-registers/standards-for-accredited-registers/accredited-registers-evidence-framework-for-standards.pdf?sfvrsn=55f4920_9

The Panel noted the findings of the ICO in relation to the three incidents it reviewed, which are not published. The Panel noted that in two of these cases, the ICO's response made recommendations to the ACC, but recognised steps it was already taking to address the incidents.

In relation to one incident however, the ICO found that the ACC had not complied with its data protection obligations. This was because personal information was inappropriately disclosed to a third party. The ICO set out further actions for the ACC to improve its information rights practices:

- All staff attend mandatory training which is routinely tested and refreshed
- All policies and procedures are updated and revised to reflect the obligations placed on controllers and processors under the General Data Protection Regulations / Data Protection Act 2018 (GDPR/DPA18)
- All data processed by the Association of Christian Councillors is subject to appropriate organisational and technical controls with regards to its security.

The ACC provided evidence for how it was addressing both the ICO's actions, and recommendations. All of the ACC's staff, assessors, Board members and Pastoral Care Trainers have been required to undertake General Data Protection Regulation (GDPR) training, and this has now been embedded into the induction process for new starters.

We reviewed the ACC's revised Data Retention Policy, and new Privacy Policy, both of which are now published on its website⁴. The ACC also reviewed all of its policies dealing with membership, complaints, and customer service to ensure they are in line with these policies. This included developing and publishing new data protection guidance for its Complaint Investigators and Panel Members, and guidelines for staff on responding to a Subject Access Request (SAR). There is now guidance for staff on how to recognise and respond to a potential data breach.

In relation to organisational and technical security controls, all staff, Board members and assessors have ACC email addresses, and are required to use its document storage systems rather than personal devices. There are secure passwords in place for accessing databases. It has appointed a third-party supplier to manage its office systems and network security. The ACC has also purchased redaction software, to reduce the risk of inappropriate disclosure of personal data.

The Panel found that the ACC had responded to the ICO's findings by taking immediate steps to improve its data security arrangements and reduce the risk of future data breaches, in line with the ICO's requirements. The Panel did not therefore think that Conditions of accreditation were required. However, it emphasised the importance of the ACC embedding these processes at every level throughout the organisation, and making sure that it has mechanisms for keeping staff up to date with any changing requirements in relation to information security.

The Panel issued the following Recommendation:

⁴ [ACC Privacy Policy.pdf \(acc-uk.org\)](#)

Recommendation One: The ACC should monitor and evaluate the implementation and integration of the new processes they have introduced to meet the requirements of the Information Commissioner's Office (ICO) in relation to information security.

We will check on progress against this Recommendation at the ACC's next assessment.

Impact assessment

The actions the ACC is taking to improve the way it deals with personal information that it is responsible should lead to better protections of the rights of data subjects, which include the right to access, under the Data Protection Act 2018⁵.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR), which helps make sure that those responsible for using personal data follow the 'data protection principles'. These principles include that the information is used fairly, lawfully and transparently; and handled in a way that ensures appropriate security. Information relating to health is considered sensitive information.

⁵ <https://www.gov.uk/data-protection>