CHURCHES' LEGISLATION ADVISORY SERVICE

140-148 Borough High Street, London, SE1 1LB
T: 020 7222 1265 E: info@churcheslegislation.org.uk
www.clas.org.uk

CLAS CIRCULAR
2026/07 (27 April)

Disclaimer

CLAS is not qualified to advise on the legal and technical problems of members and does not undertake to do so. Though we take every care to provide a service of high quality, neither CLAS, the Secretary nor the Governors undertakes any liability for any error or omission in the information supplied.

It would be very helpful if members could let us know of anything that appears to indicate developments of policy or practice on the part of Government or other matters of general concern that should be pursued.

FAITH AND SOCIETY

Advice on AI cyber threats

For information and possibly for action

Last week, the Government published an open letter to businesses on AI cyber threats. In brief, it is urging businesses to take cybersecurity seriously, to sign up to Cyber Essentials – the government-backed certification scheme that protects against the most common attacks – and to follow the advice of the National Cyber Security Centre and sign up to its Early Warning Service.

Cybersecurity is just as important for churches and voluntary organisations, and the Chairman therefore suggested that we should bring the Government's advice to the attention of CLAS members.

The full text of the letter is below:

"We are writing to you because the threat your business faces in cyberspace is changing, and the way we respond must change with it.

For years, the most serious cyberattacks have relied on a small number of highly skilled criminals. That is now shifting. A new generation of AI models are becoming capable of doing work that previously required rare expertise: finding weaknesses in software, writing the code to exploit them, and doing so at a speed and scale that would have been impossible even a year ago.

Last week, AI firm Anthropic announced a new model called Mythos. Testing by DSIT's AI Security Institute (AISI) – one of the world's leading bodies for evaluating the capabilities of Frontier AI – has found it to be substantially more capable at cyber offence than any model we have previously assessed. Recent tests of advanced AI models, including the AISI's evaluation of Anthropic's Mythos, indicate that AI cyber capabilities are accelerating even faster than had been previously envisaged. The AISI assess that frontier model capabilities are doubling every 4 months, compared to every 8 months previously. This finding is significant both for what it means today, but also because it highlights the speed at which AI capabilities are increasing and the threats they potentially pose. OpenAI also announced scaling up their Trusted Access for Cyber program last night, showing that AI's accelerating impact on cyber is not isolated to a single company, and we expect more to follow. The trajectory is clear and therefore it is vital that we are prepared for frontier AI model capabilities to rapidly increase over the next year, and plan accordingly for that outcome.

The UK is not standing still in response to this threat. We have built the AI Security Institute, the most advanced capability of any government in the world for understanding

frontier AI systems. This ensures that your government can have an independently verified, robust assessment of current capabilities.

More broadly, the National Cyber Security Centre, part of GCHQ, is world-leading in defending the UK online, and continues to publish practical guidance every business can use. The **Cyber Security and Resilience Bill**, which is currently progressing through Parliament, will strengthen protections for critical services – from the NHS to the energy system – that we all rely on, and shortly we will publish the National Cyber Action Plan setting out the steps this government will take to ensure the UK's national security against cyber threats.

Government action alone will not be enough. Every business in the UK has a part to play. Criminals will not just target government systems and critical infrastructure. They will target ordinary companies, of every size, in every sector. Attackers go where defences are weakest.

The steps organisations should take to protect against AI-driven cyber threats are the same cyber hygiene measures recommended for traditional cyber threats. We are asking every business leader reading this to take the following steps:

1. Take cyber security seriously, at the very top of your organisation.

If your board has not recently discussed cyber risk, do so at your next meeting and then regularly. This is not an issue to delegate to your IT team and forget about. This will only become increasingly important. We urge you and your board to use the **Cyber Governance Code of Practice** to ensure your organisation is sufficiently protected. Smaller businesses should also use the NCSC's Cyber Action Toolkit to help them build their cyber protection. Not all incidents can be prevented, so you should plan and rehearse how your organisation would respond to a significant incident, including consideration of how cyber insurance can support response and recovery. Free cyber insurance is available to small organisations that obtain Cyber Essentials.

2. Get the basics right with Cyber Essentials.

Most successful cyber-attacks exploit simple weaknesses: outdated software, weak passwords, missing backups. **Cyber Essentials** is the government-backed certification scheme that protects against the most common attacks. Organisations that hold it are significantly less likely to suffer a damaging cyber incident. For most businesses, getting certified is neither expensive nor difficult. You should also look to embed Cyber Essential requirements across your supply chains, and large organisations should use the NCSC's Cyber Assessment Framework.

3. Follow NCSC advice and sign up to their Early Warning Service.

The **National Cyber Security Centre** (NCSC) provides free, practical advice, training and guidance at ncsc.gov.uk for organisations of every size. Advice will also be issued by Regulators for regulated sectors. Early Warning is a free service from NCSC that can inform organisations of potential cyberattacks and give them invaluable time to act before an incident escalates.

We are entering a period in which the pace of technological change may test every institution in the country. The businesses that act now – that treat cyber security as an essential part of running a modern company, not an optional extra – will be the ones best placed to thrive through it and seize its advantages. We urge you to be among them."

Yours sincerely,

The Rt Hon Liz Kendall MP
Secretary of State for Science, Innovation and Technology

Dan Jarvis MBE MP
Security Minister, Cabinet Office and Home Office

[Source: Department of Science, Technology and Innovation, 15 April]