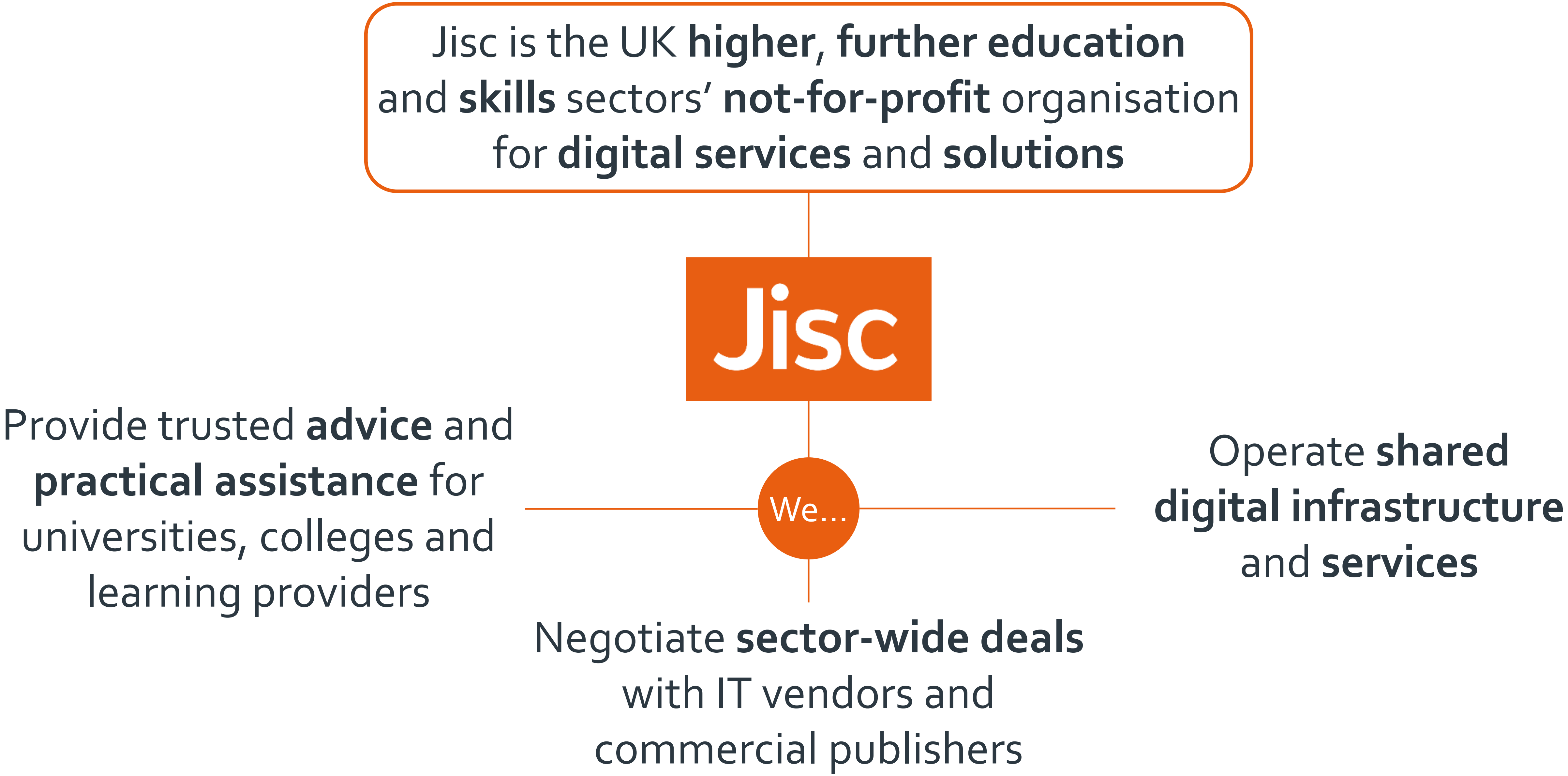
9 May 2018

Prevent Duty Update

Rohan Slaughter – Subject Specialist

Who we are?



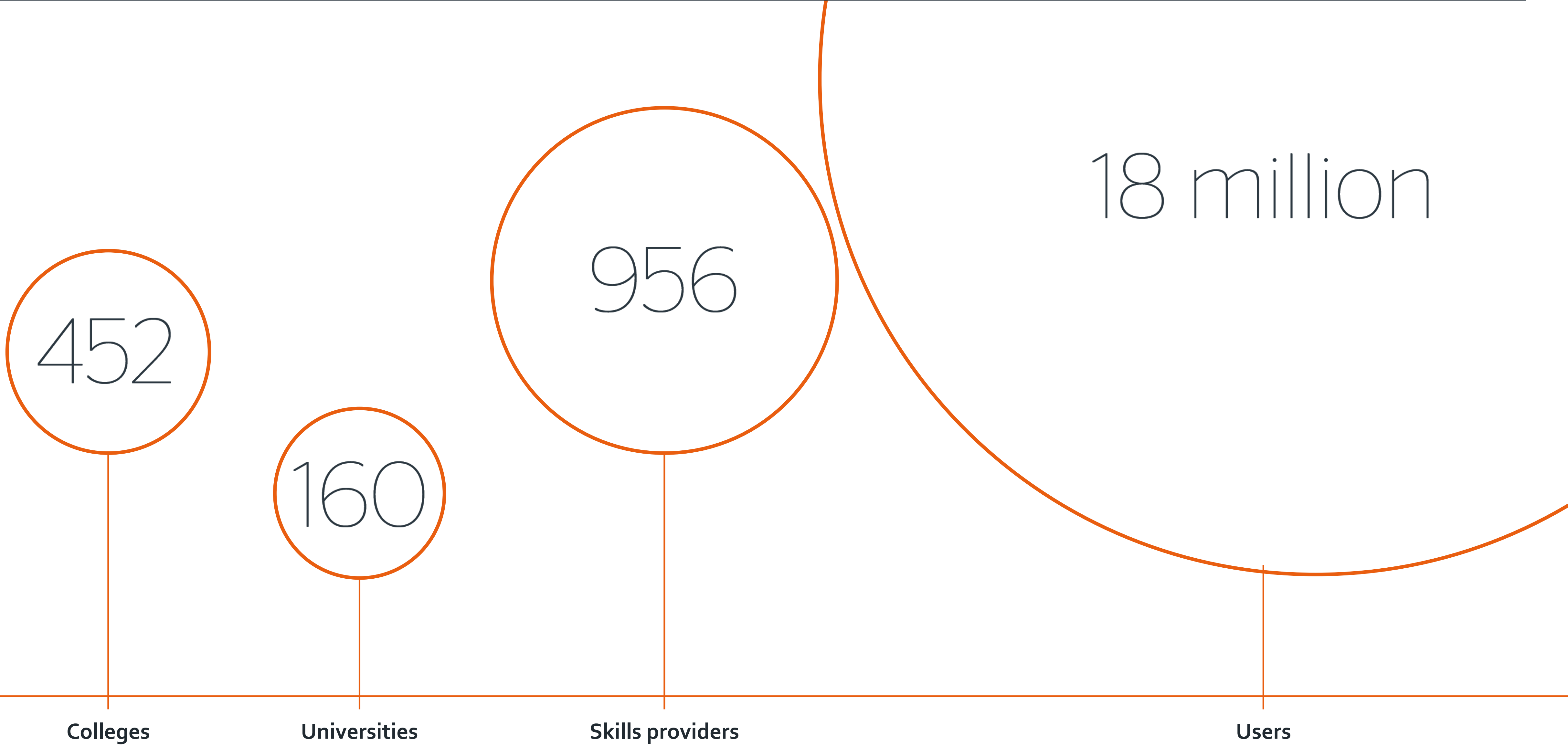
Jisc is the UK **higher**, **further education** and **skills** sectors' **not-for-profit** organisation for **digital services** and **solutions**

Provide trusted **advice** and **practical assistance** for universities, colleges and learning providers

Operate **shared digital infrastructure** and **services**

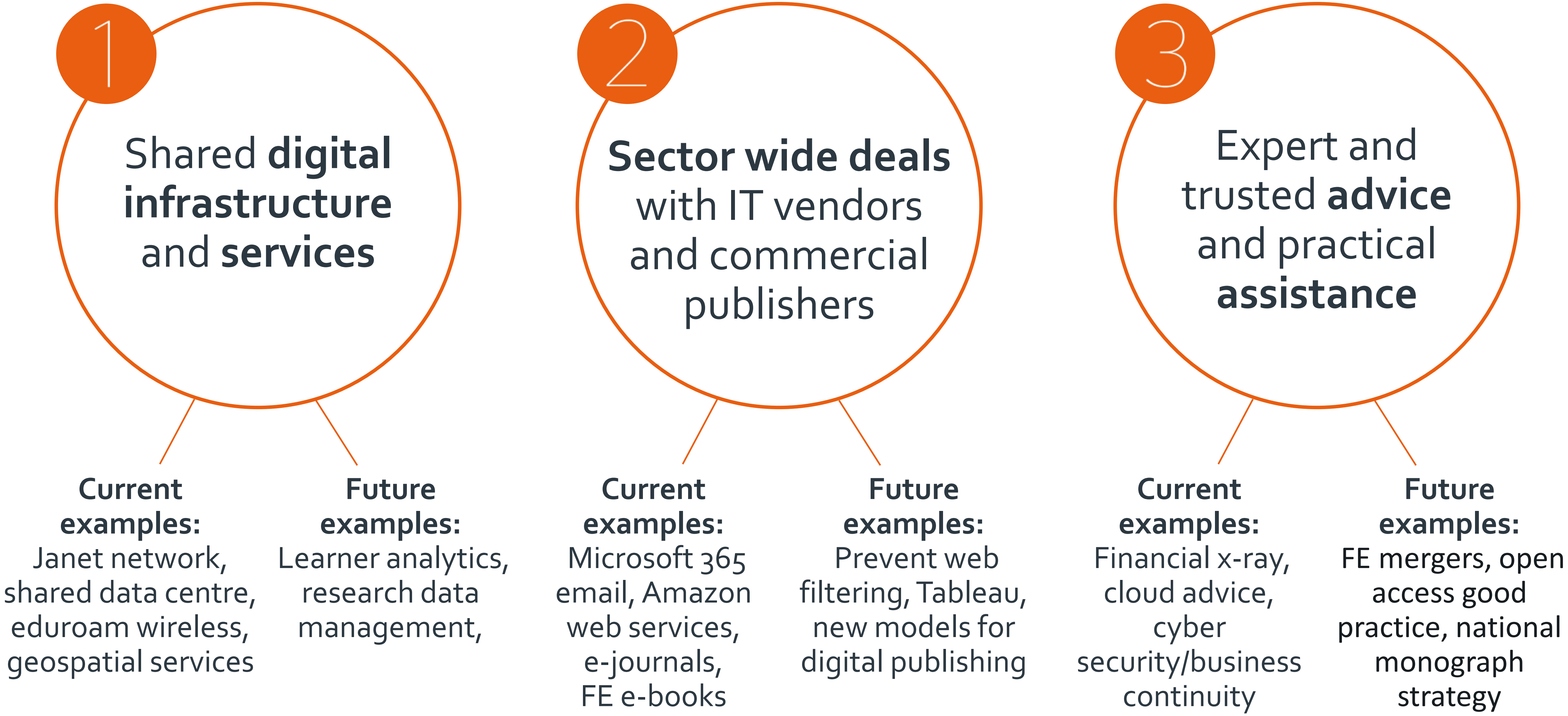
Negotiate **sector-wide deals** with IT vendors and commercial publishers

Our customers and users



452	Colleges
160	Universities
956	Skills providers
18 million	Users

We do… 3 main things



1

Shared **digital infrastructure** and **services**

Current examples: Janet network, shared data centre, eduroam wireless, geospatial services

Future examples: Learner analytics, research data management,

2

Sector wide deals with IT vendors and commercial publishers

Current examples: Microsoft 365 email, Amazon web services, e-journals, FE e-books

Future examples: Prevent web filtering, Tableau, new models for digital publishing

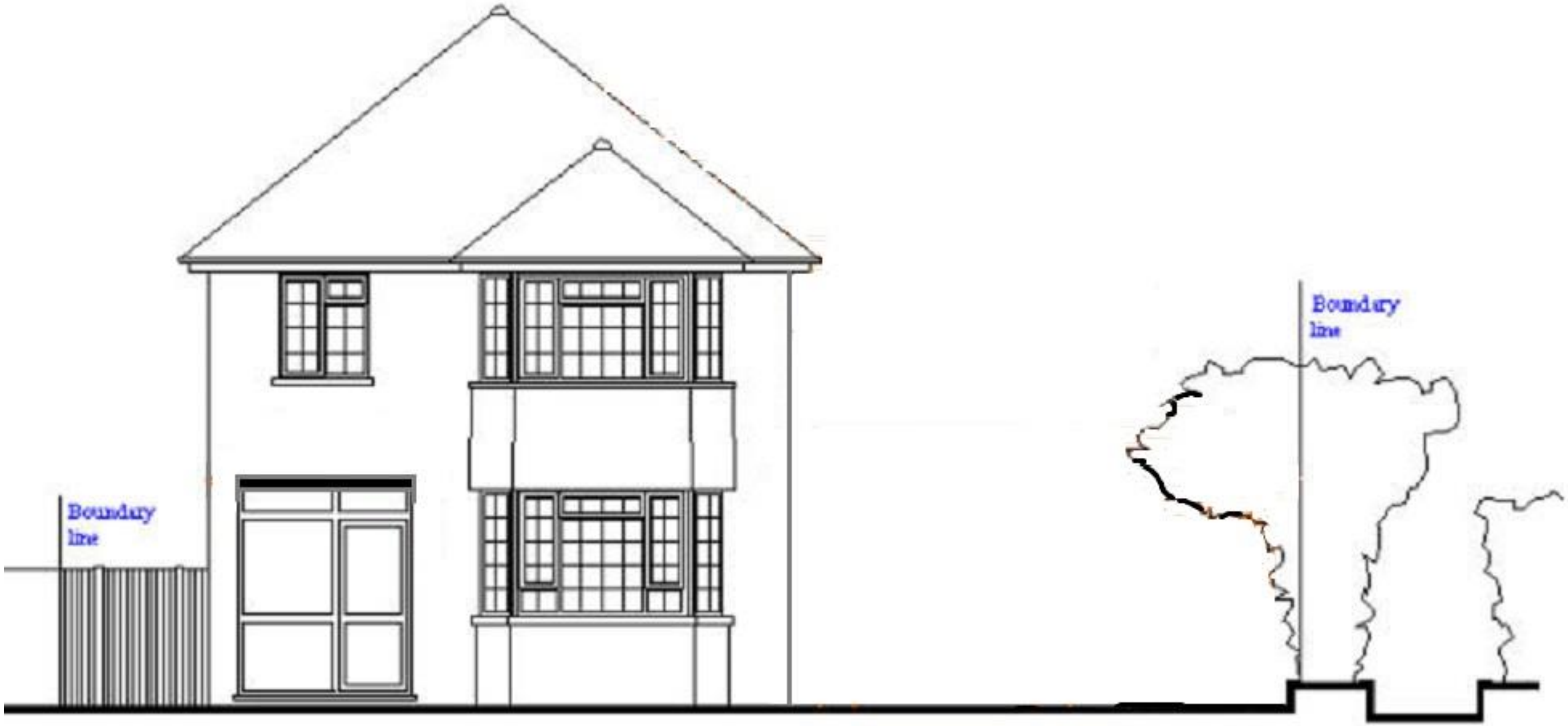
3

Expert and trusted **advice** and practical **assistance**

Current examples: Financial x-ray, cloud advice, cyber security/business continuity

Future examples: FE mergers, open access good practice, national monograph strategy

32 Safeguarding Street



Here’s the Home Office guidance for England & Wales HE – others are similar

HM Government

Prevent Duty Guidance: for higher education institutions in England and Wales

Prevent Duty Guidance for higher education institutions in England and Wales 3

This sector specific guidance for higher education institutions in England and Wales subject to the Prevent duty is additional to, and is to be read alongside, the general guidance contained in the Revised Prevent Duty Guidance issued on 16th July 2015

Higher education

4 Prevent Duty Guidance for higher education institutions in England and Wales

Prevent Duty Guidance for higher education institutions in England and Wales 5

IT policies

We would expect RHEBs to have policies relating to the use of their IT equipment. Whilst all institutions will have policies around general usage, covering what is and is not permissible, we would expect these policies to contain [illegible] educational institutions already use filtering as a means of restricting access to harmful content, and should consider the use of filters as part of their overall strategy to prevent people from being drawn into terrorism.

Monitoring and enforcement

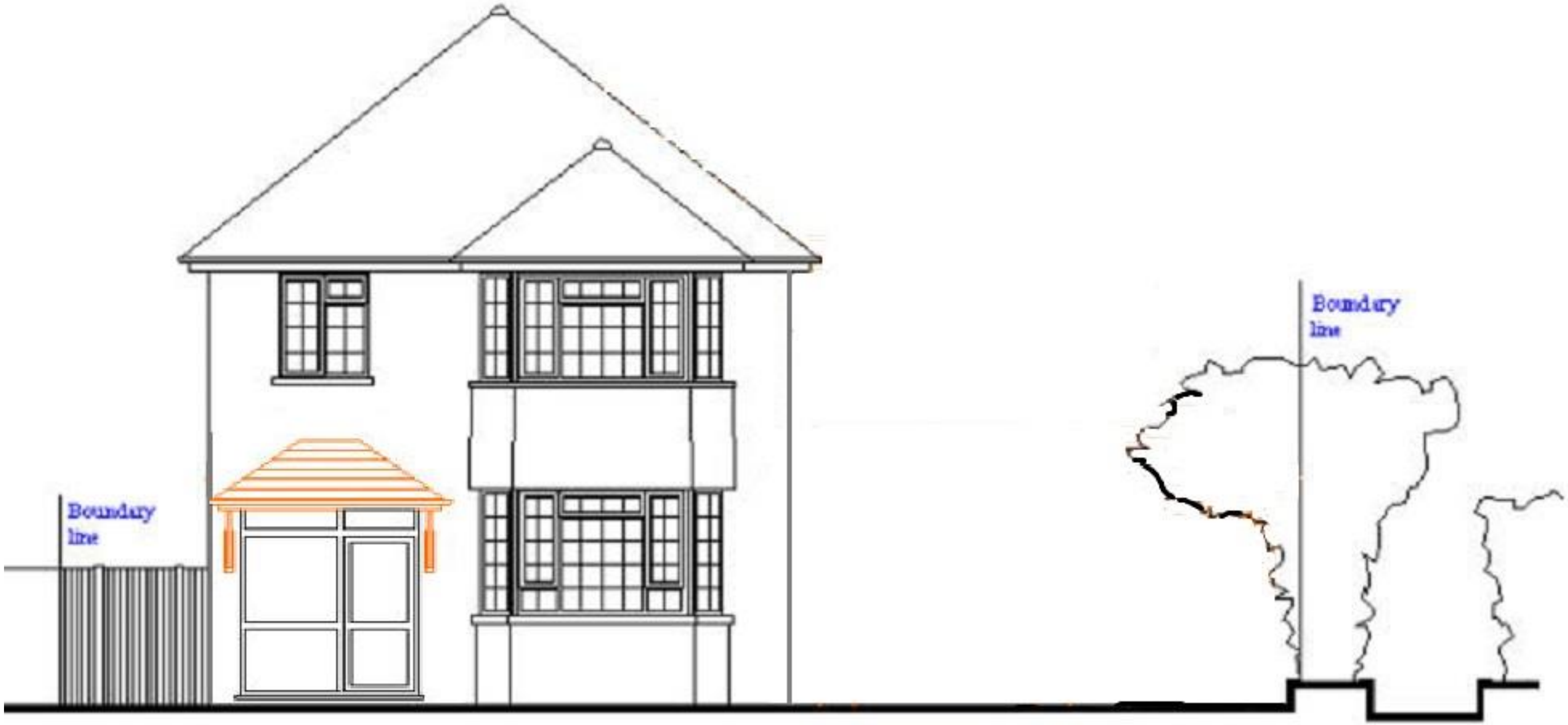
Home Office Guidance - Filtering

“Many educational institutions already use filtering as a means of restricting access to harmful content, and should consider the use of filters as part of their overall strategy to prevent people being drawn into terrorism”

Prevent Duty Guidance England & Wales

- The ‘Prevent’ duty requires providers to have:
  - appropriate policies and procedures in place for the management of external speakers and events
  - active engagement with partners, including the police and BIS ‘Prevent’ coordinators
  - a risk assessment that assesses where and how learners are at risk of being drawn into terrorism, and an action plan designed to reduce such risks
  - appropriate training and development for principals, governors, leaders and staff
  - welfare and pastoral/chaplaincy support, including widely available policies for the use of prayer rooms and other faith-related facilities
  - **IT policies that make specific reference to the ‘Prevent’ duty and relate to the use of IT equipment.**

32 Safeguarding Street,
Government Town



Ofsted Papers and findings

- The Prevent Duty / Safeguarding – how can the technical infrastructure help?
- Starting with the Ofsted paper '<u>How well are further education and skills providers implementing the 'Prevent' duty?'</u>
  - Five key matters . . .

How well are further education and skills providers implementing the ‘Prevent’ duty?

1. Are providers ensuring that external speakers and events are appropriately risk assessed to safeguard learners?

2. Are the partnerships between different agencies effective in identifying and reducing the spread of extremist influences?

3. Are providers assessing the risks that their learners may face, and taking effective action to reduce these risks?

4. **Are learners being protected from inappropriate use of the internet and social media?**

5. To what extent are staff training and pastoral welfare support contributing to learners’ safety?

Ofsted Papers and findings

“In nearly half the providers, not enough had been done to ensure that learners were protected from the risk of radicalisation and extremism when using information technology (IT). **Too often, policies and procedures for the appropriate use of IT were poor or did not work in practice.**

Over a third of providers visited were not working with the Joint Information Systems Committee (Jisc) to **develop IT policies and restrict learners’ access to harmful content on websites**.

In the weakest providers, learners said they could **bypass security settings and access inappropriate websites, unchallenged by staff or their peers**. This included websites that promote terrorist ideology and that sell firearms.

<u>In one such provider, a learner had accessed a terrorist propaganda video showing a beheading.”</u>

Key finding:

Leaders in nearly half the providers visited did not adequately protect learners from the risk of radicalisation and extremism when using IT systems.

Learners in the weakest providers were able to bypass firewalls to access inappropriate websites, including those promoting terrorist ideology, right-wing extremism and the purchase of firearms.

Ofsted Papers and findings

Recommendations

The government should:

- ensure the consistency of advice and guidance provided by BIS 'Prevent' coordinators, police 'Prevent' teams and local authorities
- **through Jisc, publicise further the support available to providers to develop IT policies that counter inappropriate internet access**
- promote the support, advice and guidance available through ETF to enable providers to do more to protect learners.

Ofsted Papers and findings

Recommendations

Providers should:

- **ensure that appropriate policies and procedures are in place, and implemented effectively, to protect learners from the risks posed by external speakers and events**
- develop stronger and more supportive links with partners, including local authorities, to develop stringent information-sharing protocols and share intelligence
- ensure that risk assessments and associated action plans are of high quality and cover all aspects of the 'Prevent' duty
- provide staff training that is aligned to job roles and evaluate this to measure its impact across the organisation
- ensure that learners have a good understanding of British values and the risks and threats of radicalisation and extremism
- **refer to the 'Prevent' duty explicitly in IT policies and procedures, closely monitor learners' use of IT facilities to identify inappropriate usage, and work with partners and external agencies for additional support, information and intelligence.**

Recommendations

Ofsted should:

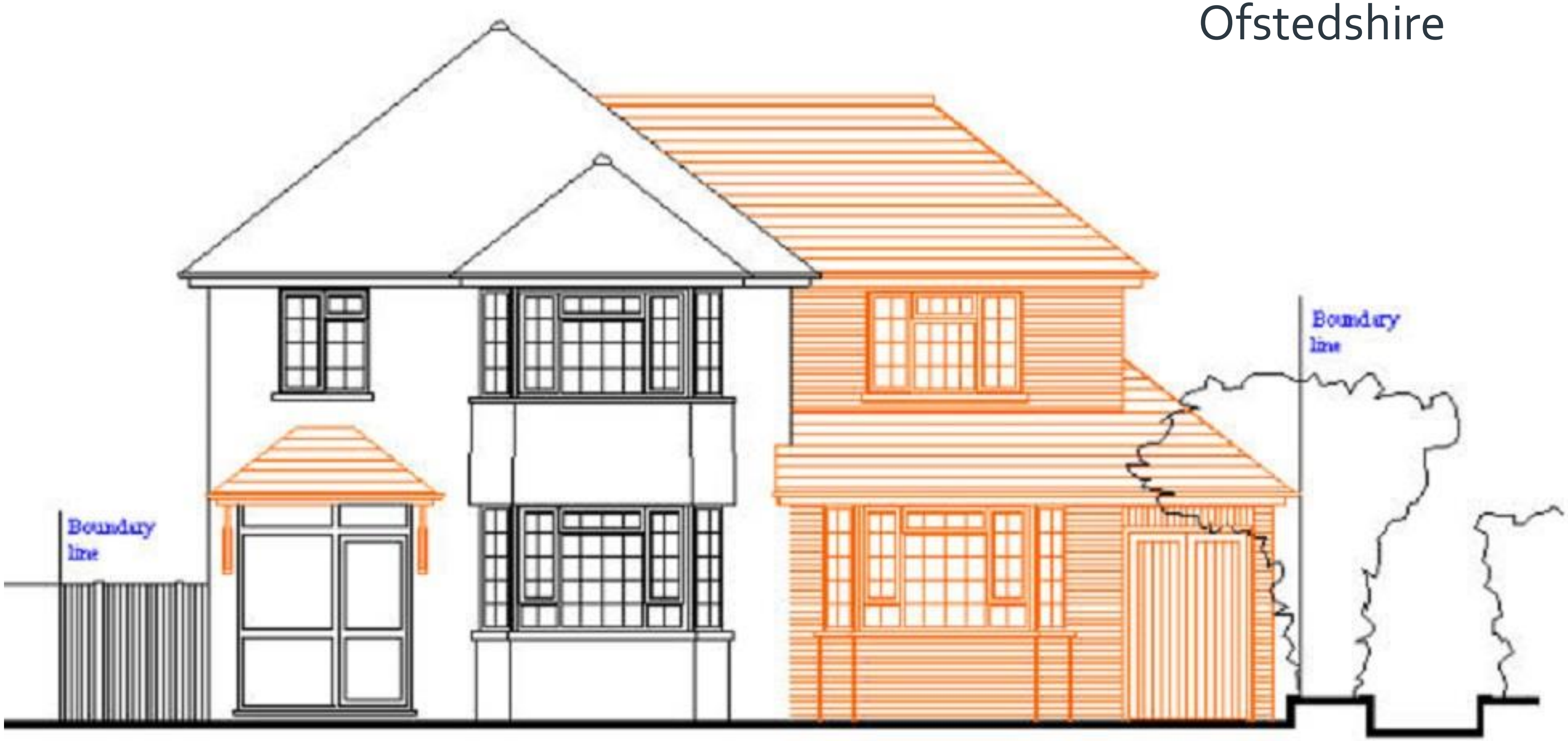
- from September 2016, **raise further its expectations of providers** to implement all aspects of the ‘Prevent’ duty, and evaluate the impact this has on keeping learners safe.

Prevent and on-line safety

- The ‘Prevent’ duty requires providers to have:
  - appropriate policies and procedures in place for the management of external speakers and events
  - active engagement with partners, including the police and BIS ‘Prevent’ coordinators
  - a risk assessment that assesses where and how learners are at risk of being drawn into terrorism, and an action plan designed to reduce such risks
  - appropriate training and development for principals, governors, leaders and staff
  - welfare and pastoral/chaplaincy support, including widely available policies for the use of prayer rooms and other faith-related facilities
  - **IT policies that make specific reference to the ‘Prevent’ duty and relate to the use of IT equipment.**

Building your Prevent Strategy

32 Safeguarding Street,
Government Town,
Ofstedshire



Ofsted – The Good

The **best providers** have liaised closely with external agencies such as Jisc and have stringent firewalls in place.

In these providers, learners reported that internet safety was strong but sometimes felt frustrated that firewalls were too restrictive. However, learners understood that it was to keep them safe while using IT.

Learners could access blocked websites if they provided the IT team with reasons for accessing the sites: for example, research for history, politics, theology or public services.

Ofsted – The Bad

IT policies and their impact on learner safety

- Leaders in 16 of the providers visited did not adequately protect learners from the risk of radicalisation and extremism when using IT systems
- Almost all the providers had an IT policy in place. However, 11 of these policies did not make explicit reference to 'Prevent' and did not work effectively in practice. As a result, learners could access inappropriate internet content.
- Monitoring of learners' use of IT varies considerably across providers, with 10 of the providers visited not monitoring IT usage adequately. Some providers did not monitor IT usage at all, while others' reports were so generic that they were of little use in identifying inappropriate IT use.
- More than a third of providers did not liaise with external agencies such as Jisc to develop IT policies and firewalls. Jisc provides guidance and support to further education and skills providers in writing IT policies and in developing firewalls for computer systems. It is named specifically in the 'Prevent' duty guidance.

Ofsted – The way forward

» The best providers visited had a range of strategies in place to ensure that learners were safe while using IT. These strategies included:

- closely monitoring IT usage in real time, in order to identify and address inappropriate use of IT, at which computer and by whom
- tracking IT use on guest log-ins
- risk-rating learners and sampling IT access
- daily reports to senior leaders of attempts to access inappropriate websites
- developing stringent firewalls with external providers
- sharing data regarding ‘popular’ contentious and blocked websites that learners had attempted to access with police ‘Prevent’ teams as part of local intelligence gathering.

Ofsted – The way forward

- Web Filtering and Monitoring is now **expected best practice**
- Technical systems **cannot** exist in isolation:
  - Safeguarding policy / practice
  - Prevent Duty Risk Assessment
  - IT Acceptable Use Policy
  - Staff training
  - Learner e-safety programme
  - HR [People] processes

Activity: Prevent in your context?

- What are you doing in your context?
  - What systems do you have in place?
  - What is your IT / Acceptable Use Policy overview?
  - Do you have a designated Prevent / Safeguarding link person with/in the IT team?
- Have you had a recent inspection?
  - What was the experience around Prevent?
  - Any useful points to share?

We don't, it's a common myth

Jisc web filtering and monitoring framework

- Jisc web filtering and monitoring framework
  - Launched Early summer 16
  - 7 contracts from the framework so far – lots of enquiries, increasing interest from all sectors
  - Case study, product review and information for BIS to be created from interview with West Suffolk college
  - Iboss partnership working very well – they are looking to place equipment in the SDC.
  - Web filtering customer training course developed and live
  - **the 3rd most popular service page after eduroam and Janet**

Jisc Web filtering and monitoring framework

- The Jisc Web Filtering and Monitoring Framework
- Not the same thing as the old 'web filtering service'
- Benefits over 'old service':
  - Options for cloud-based, local hardware-based and hybrid products
  - Ability to monitor, both with and without filtering
  - Ability to create and export reports on user activity
  - Ability to set different rules and categories for what different groups of students/staff can/cannot access
- Suppliers:
- Comtact (ZScaler), BSIGroup (ZScaler), Gaia Technologies (SmoothWall), Iboss Cybersecurity (iBoss), Insight (Smoothwall), Pinacl Solutions (SmoothWall), Softcat (CensorNet)

Other options . . .

- There are other options . . . .
- Standalone Appliances
  - Lightspeed
  - Websense
  - Sophos
- Firewall based
  - Smoothwall
  - Fortigate
  - SonicWALL
  - Sophos
  - WatchGuard
- Free and Open Source solution
  - Dans Guardian

Advice after the Ofsted paper

- **Policy** - ensure that you create a policy on web filtering and ensure that all agreements are updated to reflect this. Policy is usually decided at an organisational level, you should also use the policy to inform the configuration of the Web-Filtering, rather than being led by an IT Service (internal or external).
- **Identity** - ensure that the organisation is issuing users with a unique user account, so that accountability is possible. It also enables you to offer ‘granular access’ meaning different levels of access for different groups of users.
- **Accountability** - All organisations should have good accountability for their users Internet access. This is usually done through some sort of logging e.g. at a Firewall or via a Web-Filtering appliance

Advice after the Ofsted paper

“Common mistakes and how to deal with them”

- Accountability: All of your students and staff must have individual user accounts
  - Group accounts are a very bad idea
  - Classroom accounts are an even worse idea
- Web Filtering is part of safeguarding your learners
  - If you don’t screen out the worst of the content learners could find it by accident
  - Duty of Care . . .
  - Mental Capacity Act . . .
  - Risk Assessment . . .
  - Check out the quality of the web filtering system that you have in place

Advice after the Ofsted paper

- Web Monitoring lets you know what people are doing, only if:
  - It is working properly and if it is actually turned on
  - If it is any good
  - If you doing anything with the data, also how long do you keep the data for, is this ok?
- Often desktops / laptops are covered, but what about mobile devices?
  - Tablets and other mobile devices are sometimes treated differently
  - This can be because you have an older system that cannot deal with them
  - This can be because the web filtering and monitoring systems were setup to be ‘Windows specific’

Advice after the Ofsted paper

Questions to ask with your IT team:

- Do all our staff and students have individual user accounts?
- Do we have a web filtering system in place?
  - Is it any good?
- Do we have web monitoring in place?
  - Where in our policies is this noted?
  - Are we actually doing what we say we are doing?
- Our we supporting the users (staff and students) correctly?
  - Do they feel comfortable coming to us?
  - Do they understand we are looking out for them?

Advice after the Ofsted paper

- Are we looking at our logs . . . ever?
  - What is being logged?
  - Is this useful?
  - Who is looking at the logs?
  - Under what circumstances are the logs being reviewed?
  - Have we communicated this properly?
- Are all of our connected devices subject to filtering and monitoring?
  - Yes even the iPads . . .
  - And the random Android equipment . . .

A little more...

RED button live on the Jisc Website

- »cyber security page
- »Prevent training pages

‘Red STOP Button’

REPORT
ONLINE
TERRORIST
& EXTREMIST
MATERIAL
HERE

Current Security products and services

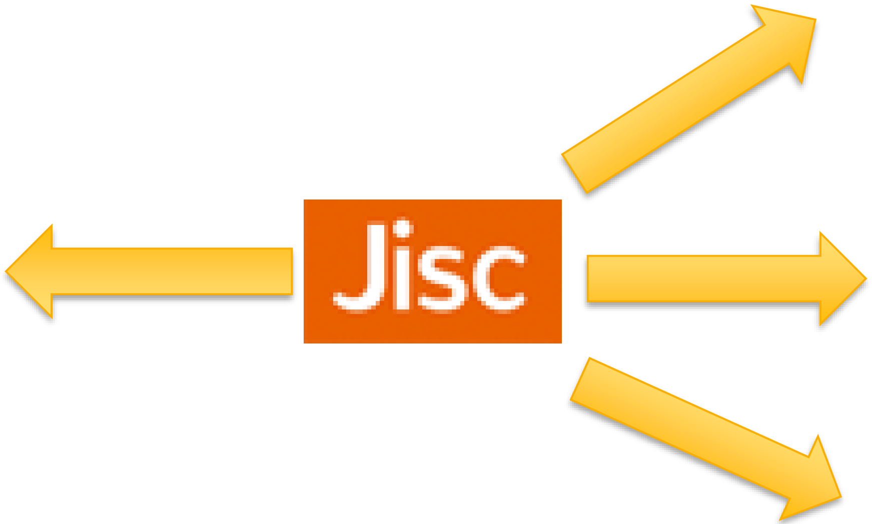
- Janet network CSIRT
- Web filtering and monitoring
- Vulnerability assessment and information
- Manual penetration testing
- Email abuse protection
  - Spam-relay tester and notification system
  - Security blacklists and whitelists
- WRAP and security courses

www.jisc.ac.uk/network/security

Jisc

Jisc - Training

HM Government



Workshop to Raise Awareness of Prevent (WRAP)

Filtering and monitoring: how can they help?

Information security policies

Many, many more courses

Training - Workshop to raise awareness of Prevent (WRAP)

WRAP is a free specialist workshop, designed by HM Government to give you:

- An understanding of the Prevent strategy and your role within it
- The ability to use existing expertise and professional judgment to recognise the vulnerable individuals who may need support
- Local safeguarding and referral mechanisms and people to contact for further help and advice.
- This workshop is an introduction to the Prevent strategy , it does not cover wider institutional responsibilities under the duty.

Jisc

Jisc WRAP Training Update

- Total people who have completed WRAP training with Jisc is now 3343
- The sector breakdown is:
- 34% Publicly funded HE,
- 49% Skills (SFA or WAG contract),
- 8% Publicly funded FE,
- 1% Alternative providers/Independent training providers,
- 5% Local Authorities (ACL and skills),
- 3% Other.
- Further session dates in the schedule
- Sessions take place on Tuesday, Thursday, Friday – 3 sessions a week and are experiencing high demand for courses from all sectors – courses are fully booked for 2 weeks in advance of delivery.

Training - Filtering and monitoring: how can they help?

The course is designed for anyone considering or reviewing the use of filtering and monitoring technologies to implement organisational policies. No experience with networking technologies is required, but it would be an advantage to have a foundation knowledge

Details are available on the website

Next
Filtering and Monitoring Online course to
take place on 10, 17 and 24 July 2018 (online course over three sessions)

Training - Information security policies

Topics covered

- » Recognising risks
- » Analysing risks
- » Treating risks
- » From risks to policies
- » Managing information security
- » Policies and the organisation

Training

- Facilitated online learning, no travel required
- Delivered by our award winning training team
- Highly participatory sessions
- Share best practice across the sectors and nationwide

- Information and registration at jisc.ac.uk/advice/training

Learning & Performance Institute
Accredited Learning Provider

ETF resources

- Prevent for Further Education and Training
- Guidance materials are provided
  - Inclusive of the Jisc document 'Web filtering and monitoring: Guidance for the further education and skills sector in the context of the Prevent Duty'
  - This is a Jisc document that is based in part on an earlier version of this presentation
  - Useful to share with your IT team.

Thank you – any questions?

Rohan Slaughter
Subject Specialist

Twitter @rohanslaughter

M 07468 727047

rohan.slaughter@jisc.ac.uk

jisc.ac.uk

Security - GOV.UK cyber pages

- Keeping the UK Safe in Cyberspace sets out the policy context for UK cyber;
  - https://www.gov.uk/government/policies/cyber-security
- 10 Steps to Cyber Security
  - https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility
- BIS advice for small businesses
  - www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know
- Cyber Essentials
  - www.cyberstreetwise.com/cyberessentials
- Centre for the Protection of National Infrastructure (CPNI)
  - www.cpni.gov.uk/advice/cyber
- Cyber Streetwise
  - www.cyberstreetwise.com
- Get Safe Online
  - www.getsafeonline

Jisc Cyber Security Services

- Explore the security support available to those connected to the Janet Network https://www.jisc.ac.uk/network/security
- Janet computer security incident response team (CSIRT)
  - https://www.jisc.ac.uk/csirt
- web filtering service
  - https://www.jisc.ac.uk/web-filtering
- Mailer Shield
  - https://www.jisc.ac.uk/mailer-shield
- education shared information security service (ESISS)
  - https://www.jisc.ac.uk/esiss
- Email advice and testing
  - https://www.jisc.ac.uk/email-advice
- Blacklists and whitelists
  - https://www.jisc.ac.uk/blacklists
- Jisc Certificate Service
  - https://www.jisc.ac.uk/certificate-service

Useful Prevent Links

If you want to know more

» Link to Andrew's blog

https://community.jisc.ac.uk/blogs/regulatory-developments/article/prevent-duty-fehe-current-position-july-2015

» Prevent duty guidance

https://www.gov.uk/government/publications/prevent-duty-guidance

» The Statutory Instrument bringing it into force is The Counter-Terrorism and Security Act 2015 Regulations 2015 at http://www.legislation.gov.uk/uksi/2015/928/contents/made

Useful Policy Links

- https://www.jisc.ac.uk/guides/networking-computers-and-the-law/network-monitoring

- http://www.ucisa.ac.uk/modelregs

- https://community.jisc.ac.uk/library/acceptable-use-policy

- https://community.jisc.ac.uk/library/janet-policies/security-policy

- https:/community.jisc.ac.uk/library/janet-policies/eligibility-policy