Web filtering and monitoring

Guidance for the further education and skills sector in the context of the Prevent Duty

Background

This paper has been produced following discussion between the Department for Education, the Education and Training Foundation and Jisc staff.

It became clear at a number of Prevent themed events that it would be useful to produce a guidance document to complement presentation materials that have already been made available to the sector. Note that this paper only applies to further education (FE) and skills providers in England and Wales that are **Education and Skills Funding Agency (**ESFA) funded providers, which also includes independent learning providers, those funded through the apprenticeship levy and the adult education budget These notes do not apply to higher education providers, but the notes may be of use to HE providers where they have ESFA funded students, or students under 18.

It is noted that this paper has been informed by the Ofsted survey **How well are further education and skills providers implementing the Prevent duty?** alongside the direct feedback of IT managers, Ofsted nominees and other managers from colleges that have had recent Ofsted inspections.

The Prevent Duty is a specific set of responsibilities placed onto higher education, further education and skills providers. The Counter-Terrorism and Security Act 2015 contains a duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism. The duty came into force on 18th September 2015 for further education. For other affected sectors the Prevent Duty came in on 1st July 2015 (this includes schools and local authorities). The Prevent Duty does not apply in Northern Ireland. Compliance with the Prevent Duty for publicly funded further education and skills providers in England is now monitored by Ofsted inspections, **under the common inspection framework applying to inspections from September 2015.** The protection of learners and staff from the dangers of radicalisation and extremism is an aspect of safeguarding. Safeguarding is inspected as part of the **effectiveness of leadership and management key judgement**.

This document is structured thus: Firstly the Ofsted survey is examined alongside the statutory Prevent Duty Home Office guidance for further education and skills providers in England and Wales that relates to IT matters generally and web filtering and monitoring specifically. A section follows on how web filtering and monitoring fits in with the wider requirements the Prevent Duty. A section detailing what support Jisc can provide is presented followed by advice and guidance on what needs to be considered when implementing web filtering and monitoring including what to avoid, and example questions to ask with IT teams. Finally additional related services and links to other sources that the reader can go to for support are provided.

This paper has been prepared by Jisc subject specialist **Rohan Slaughter** with support from **Nelson Ody**, Security Services Manager at Jisc. Note that this paper is for general advice and guidance only and does not constitute legal advice. Readers are strongly advised to read the government guidance directly and it is noted that the content of this document is based on our understanding of the relevant official guidance.

Contents

Home Office guidance and the Ofsted survey

The Ofsted survey **How well are further education and skills providers implementing the Prevent duty?** is a useful place to start in analysing Ofsted's early findings on implementation from November 2015 to May 2016 following the government issuing the **Prevent Duty Guidance** in September 2015 and specifically the **Prevent duty guidance for further education institutions in England and Wales**.

Home Office guidance

The government **Prevent duty guidance for further education institutions in England and Wales** is quite brief when discussing how IT system might assist with addressing the Prevent Duty:

> *IT policies*
>
> *26. We would expect institutions 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 that all policies and procedures will contain specific reference to the duty. 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 from being drawn into terrorism.*
>
> *27. Institutions must have clear policies in place for students and staff using IT equipment to research terrorism and counter terrorism in the course of their learning.*
>
> *28. The Joint Information Systems Committee (JISC) can provide specialist advice and support to the FE sector in England to help providers ensure students are safe online and appropriate safeguards are in place. JISC also has a Computer Security Incident Response Team who can provide assistance in the event of an online incident occurring. Monitoring and enforcement*

ACTION: In response to the above guidance all providers should ensure that all IT policies include a specific reference to the Prevent Duty and how this relates to the use of IT equipment and services.

Ofsted survey

The Ofsted survey **How well are further education and skills providers implementing the Prevent duty?** Sets out in greater detail what inspectors are looking for in FE and skills contexts. Note that it is understood that this guidance applies to all ESFA funded general further education colleges, independent specialist colleges and skills providers inclusive of independent learning providers, those funded through the apprenticeship levy and the adult education budget. Please note that all emboldening below is Jisc's.

One of five key matters covered in the Ofsted survey is "**Are learners being protected from inappropriate use of the internet and social media?"**

The survey found:

> "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.
>
> **In one such provider, a learner had accessed a terrorist propaganda video showing a beheading."**

The Prevent Duty guidance specifically mentions Jisc as a source of specialist support and advice to help providers ensure learners are safe online and appropriate safeguards are in place.

ACTION: consider seeking advice on both the policies in use and the security features of your network from your Jisc Account Manager who can access the Jisc subject specialist team for more specific advice, guidance and, if needed, dedicated consultancy services.

The survey continues with the following 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."

A number of recommendations were made by Ofsted, the following are extracts from the survey.

The government should:

- **"through Jisc, publicise further the support available to providers to develop IT policies that counter inappropriate internet access"**

Providers should:

- "**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"**

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."

Examples of good practice from the Ofsted survey

"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."

Examples of poor practice from the Ofsted survey

"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."

Department for education guidance

In reference to the Keeping Children Safe in Education statutory duty (September 2016), the Department for education (DFE) has produced statutory guidance **Keeping children safe in education: for schools and colleges**. Specific reference is made to how web filtering and monitoring can be used and additional guidance is provided in Annex C of the document.

How web filtering and monitoring fits in with the wider institutional response

- Based on the above Ofsted survey extracts, web filtering and monitoring is therefore seen as **good practice that is expected by Ofsted. In addition Jisc and DfE also note that web filtering and monitoring is seen as good practice in this context**
- Note that Ofsted has made more explicit what it's good practice expectations are in the context of the Home Office Prevent Duty guidance document
- Note that the section below 'Web filtering and monitoring: things to consider' covers how you might go about implementing a system that is likely to be suitable
- However the technical systems cannot exist in isolation and the following must be considered:
  - Safeguarding policy/practice
  - The Prevent Duty risk assessment
  - The institution's IT acceptable use policy (AUP)
  - The staff training programme
  - The learner e-safety programme
- Human resources (people) processes should be included

The provision of a web filtering and monitoring system can now be seen as **good practice in further education and skills** as part of meeting the expectations of the **Prevent Duty.**

Web Filtering specifically covers the filtering of content, generally this is to block access to inappropriate content, and web monitoring provides a system to log access to the internet. It is important to note that the measures implemented by an organisation are only effective whilst users are actually accessing the internet via the organisation's systems. Should a user who is using their own device switch over to using 3G/4G mobile networks there will be no visibility of this web traffic.

Web monitoring systems make a record of a user's web activity. Such systems will record to differing levels of detail but in essence they record the web pages visited, the search terms used on search engines and any files that may be downloaded or accessed. It is possible to retain this data for differing lengths of time, this retention period can be determined by the type of system in place. Note that most systems allow for the generation of both automatic reports (sometimes called 'surface logs') as well as the generation on request of logs of a specific user's activity, perhaps over a given time period.

Based on the Ofsted survey **The Prevent duty in further education and skills providers** that has been discussed above, recent Ofsted reports and feedback from colleagues in the sector, it is felt very likely that for providers without web filtering and monitoring in place, they will be found unable to fully discharge the Prevent Duty. Appropriate web filtering and monitoring and proportionate policies and procedures are expected to be in place to safeguard learners.

It is possible that this issue may seriously impact on any future Ofsted grade at a college if not addressed as part of the usual technology strategy and safeguarding policy/practice normally undertaken in colleges. A number of recent Ofsted reports have at least mentioned this area, if not had an actual focus on this area.

It is therefore recommended that all providers consider implementing a robust web filtering and monitoring system (alongside a robust safeguarding and Prevent Duty policy/risk assessment) as a priority to ensure that colleges can meet the Prevent Duty and ensure that all learners are appropriately safeguarded.

Any solution implemented should ensure that all web traffic generated by staff and learners from any device, (inclusive of mobile devices such as Apple iPads) should be both content filtered and monitored. All web traffic should be auditable and reportable to ensure that the Prevent Duty and good safeguarding practice can be followed. As a starting point all learners and staff should have unique user accounts. Note that in some providers this is not the case and without an account for each user there cannot be accountability. In addition all endpoint devices that are being used to browse the web should either be enrolled on the domain or forced to use a domain credential to perform a secondary login prior to being allowed to browse the internet.

ACTION: questions to ask in your context:

- How does our safeguarding policy and practice link into the Prevent Duty?
- How does our Prevent Duty risk assessment influence the technical response
- Where is the Prevent Duty referenced in our IT acceptable use policy and is there a designated Prevent/safeguarding link person with/in the IT team?
- What is covered in our staff training Prevent Duty programme? Is this sufficient?
- What is covered in our learner e-safety programme? Are we covering this as early as possible in the course?

Note that in IT courses or courses that require the use of IT, it is suggested that e-safety should be covered in week 1, or when user accounts are given to learners. It is suggested that good e-safety practice should be regularly covered throughout the course and that opportunities can be naturally used where the use of the internet is required as part of the course. For example teachers can suggest search terms or specific resources to learners and can build activities around the principles of e-safety.

Note that a number of providers have found it useful to create an 'e-safety incident flowchart' that shows how a concern or incident might be dealt with. This flow chart can demonstrate the decision making points, who would make such decisions and what the options might be for progressing the incident. Such a flowchart can usefully demonstrate where existing safeguarding or human resources processes can be activated and when external bodies, such as the police, should be contacted for assistance. An example flowchart is provided as Appendix A.

Jisc web filtering and monitoring service

Note that as a matter of routine the Janet network is not filtered. Jisc offer a **Web filtering and monitoring** procurement framework that was launched in early summer of 2016. It is possible for Jisc member organisations to purchase a web filtering and monitoring solution via this framework. There are a number of suppliers on the framework inclusive of:

- Comtact (ZScaler)
- Espion (ZScaler)
- Gaia Technologies (SmoothWall)
- iBoss Cybersecurity (iBoss)
- Insight (Smoothwall)
- Pinacl Solutions (SmoothWall)
- Softcat (CensorNet)

The framework offers a number of advantages:

- Preferential pricing
- 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 learners/staff can/cannot access

Jisc is able to provide support and guidance to Jisc members who are considering purchasing a web filtering and monitoring system via the framework. There is a **buyer's guide** web page available on the framework. The **scope of requirements** on the framework is available on the web site and this document details the stringent requirements that all suppliers on the framework had to meet. Advice and guidance on the framework can be provided by contacting the **Janet Service Desk**. Additional context can be provided by Jisc subject specialists via your Jisc account manager.

Jisc's **web filtering and monitoring** procurement framework provides cloud based, on-premises, and hybrid web filtering and monitoring options. This framework goes further than the original 'Jisc web filtering service' and offers a number of enhanced features over the more basic service that are detailed above. Filtering solutions can be based on locally hosted appliances and virtual servers which are likely to be suitable for providers depending on their size (number of computers/devices/users), their location and the nature of their internet connection. It is also possible to utilise a cloud based solution, and this may have certain advantages for some providers due to the multi-site/distributed nature of some of the providers.

Other commercial web filtering and monitoring products

Note that other web filtering and monitoring products exist outside of the Jisc web filtering and monitoring framework and this list is provided for reference purposes only. Note that Jisc is not endorsing these products nor asserting that these products may be suitable for a given purpose by listing them here.

- Standalone appliances
  - **Lightspeed**
  - **Websense**
  - **Sophos**
- Firewall based
  - **Fortigate**
  - **SonicWALL**
  - **Sophos**
  - **WatchGuard**
- Free and open source solution
  - **Dans Guardian**
- Managed services
  - **E-safe**
  - **Future Digital**

Web filtering and monitoring: points to consider

When putting in place a web filtering and monitoring system the most important points to consider are:

- Policy—ensure that you create a policy on web filtering and ensure that all agreements are updated to reflect this.
  - This policy should include details of the nature of the filtering and monitoring system in place, what specifically is being monitored and how long logs are being retained for.
  - The policy should set out how the logs will be used, and who will access or process them and under what circumstances.
  - 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).
  - It is important that the staff who administer web filtering and monitoring systems are operating under the terms of their organisational policy.
  - Guidelines and policy for the review and use of the resulting reports need to be considered.
- Identity—ensure that the organisation is issuing users with a unique user account, so that accountability is possible. This also enables offering ‘granular access’, i.e. 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. The reports generated from the web filtering and monitoring logs should provide the level of accountability required by the organisations policy.

It is not possible to have accountability without identity being in place. It is important that all users have their own user accounts, it is not possible to have accountability if group accounts are in use.

It is noted that in some contexts, such as LLDD (learners with learning difficulties or disabilities) units in mainstream colleges or in independent specialist colleges, that some learners may not be able to easily manage their own user account passwords. It could be that a simplified password option could be used for some learners, or an alternative option such as using a smart card to login or the Windows 10 only feature **Windows Hello** could be utilised. If it is not possible for whatever reason to change the password policy or to utilise another method of login, then it could be possible for designated staff members to have access to student passwords in order to assist learners with the management of their passwords. If this option is selected then a robust policy environment must be utilised to minimise the chances of a staff member attempting to mask their own use of the internet through the use of a student’s account. It is suggested that such activity could be considered a serious matter and dealt with via appropriate disciplinary procedures.

Web filtering can be considered part of safeguarding learners form accessing inappropriate content by accident. This is particularly relevant where staff have a duty of care for vulnerable learners. There is a place for risk assessment in determining what level of filtering may be appropriate. Part of this will be about applying the context from the Prevent risk assessment, but it may also be useful to undertake individual or group risk assessments for learners with additional support needs and apply a different filtering profile to those learners, should the infrastructure in use allow this.

It is noted that in some specialist college contexts that a full e-safety risk assessment is carried out at the time that learners are issued with user accounts. The purpose of this risk assessment is to scale the level of support that learners requires in order to make use of the internet, inclusive of social media. As part of this process web filtering can be considered.

It is useful to check out the quality of the web filtering that is in use and the **UK Safer Internet Centre** provides a set of provider self-assessments against criteria supplied by the UK Safer Internet Centre.

Web monitoring can be useful in both enforcing policy and in terms of detecting behaviour that may lead to a safeguarding/Prevent intervention. This can only be done if the monitoring system has been properly configured and is working well. It is useful to ask what is done with the data, how long it is kept for and is this appropriate to the context? It is noted that logs should be reviewed by a competent person. It is possible to tune what is logged and alerted, this may be useful if it is found that the automated system is generating a large number of false positives. It is also possible to have these 'surface logs' emailed to a designated member of staff, normally the safeguarding lead. It is noted that having busy IT staff review such logs may not be the most effective way of safeguarding learners.

It is also useful to regularly review web filtering and monitoring systems. It may be that if an older system is in use that it is performing good service in terms of the Windows desktops and laptops in an institution but it may not take full account of mobile devices or devices that are using a guest wireless system, inclusive of devices used under a BYOD (Bring Your Own Device) programme. It is noted that to be considered effective, web filtering and monitoring systems should be able to resolve all web traffic to an individual, irrespective of the device it is generated from.

It is important to ensure that the policies in use accurately describe the practice in your institution. It is a legal requirement to inform staff and learners that you are utilising web filtering and monitoring as the logs will constitute personal data under the Data Protection Act. It is also useful to describe the processes that are in use to ensure that the web filtering and monitoring system is not abused, inclusive of stating when and how an investigation might take place, and who would conduct such an investigation. It is important to explain why an organisation has put these measures in place and what they are intended to prevent or detect. It is useful to make it clear and transparent that web filtering and monitoring is in place for the purposes of safeguarding and to discharge the Prevent Duty.

ACTION: questions to ask with your IT team:

- Do all our staff and learners have individual user accounts?
- Do we have a web filtering system in place?
  - Is it meeting our needs?
- Do we have web monitoring in place?
  - Where in our policies is this noted?
  - Are we actually doing what we say we are doing?

- Are we supporting the users (staff and learners) correctly?
  - Do they feel comfortable coming to us?
  - Do they understand we are looking out for them?
- Are we looking at our logs
  - 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?
  - Inclusive of mobile devices such as iPads and Android tablets?
  - Inclusive of BYOD devices joined to the guest wireless service?

Additional sources of support

WRAP (Workshop to Raise Awareness of Prevent)

Jisc is accredited by the Home Office to deliver the **Workshop to Raise Awareness of Prevent (WRAP)** as a live online facilitated session. WRAP is a free specialist workshop, designed by the government to give you:

- An understanding of the Prevent Duty 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 Duty strategy, it does not cover wider institutional responsibilities under the duty.

Red STOP button

It may be useful for institutions to provide the 'Red Stop button' on their websites or intranets in order for learners and staff to **report online material promoting terrorism or extremism**.

Jisc resources

The Jisc **Cybersecurity page**, brings together all the services and guidance that Jisc provide around Cybersecurity. Examples include:

- Janet network **CSIRT** (Computer Security Incident Response Team)
- **Web filtering and monitoring** framework
- **Vulnerability assessment and information**
- **Manual penetration testing**
- **Email abuse protection** (**spam-relay tester and notification system**)
  - **Mailer Shield**
  - Security **blacklists and whitelists**
- Training on **Filtering and Monitoring: how can they help?**
- Jisc **certificate service**
- See Also:
  - Link to Jisc's chief regulatory advisor **Andrew Cormack's Blog**
  - Jisc Guides **Network monitoring** and **Safeguarding learners online**
  - Jisc's **acceptable use policy**
  - Janet's **security policy** and **eligibility policy**

Useful gov.uk web pages

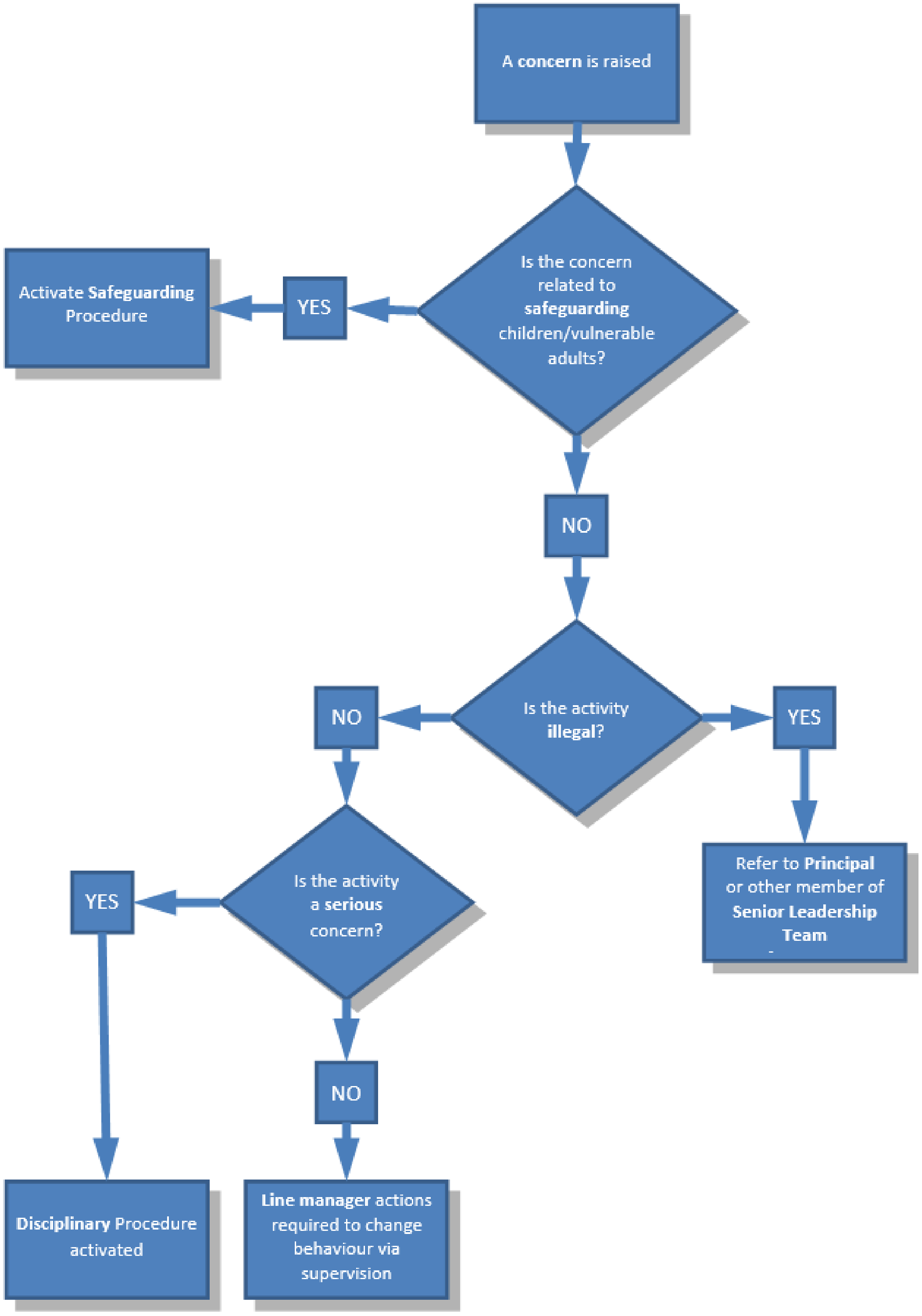
- **Prevent Duty guidance**
- **Counter Terrorism and Security Act 2015**
- **Keeping the UK safe in cyberspace**
- **10 steps to cyber security**
- **BIS advice for small businesses**

Other Sources of support

- The ETF provide the **Prevent for Further Education and Training** web site and provide a number of courses via the **Foundation Online Learning** web site
- **Cyber essentials**
- **Centre for the protection of national infrastructure** (CPNI)
- **Cyber streetwise**
- **Get safe online**

Appendix A

Example e-safety incident flowchart from a Jisc member organisation that has kindly agreed to share such. Note that each individual organisation will need to create a flowchart that reflects their context.


A concern is raised
Is the concern related to safeguarding children/vulnerable adults?
YES
Activate Safeguarding Procedure
NO
Is the activity illegal?
NO
YES
Refer to Principal or other member of Senior Leadership Team
Is the activity a serious concern?
YES
Disciplinary Procedure activated
NO
Line manager actions required to change behaviour via supervision

JEIST (Jisc Enterprise Infrastructure Sub Team) note

All information provided here is provided on an "as is" basis and is for general information only, unless the information is part of specially contracted work, in which case the terms of the corresponding contractual agreement between us shall apply. Whilst we apply a wealth of collective knowledge and experience to ensuring the accuracy and completeness of our advice and of the information we provide, we are unable to provide any representations, warranties or guarantees, whether express or implied, as regards this advice and information. It therefore remains the responsibility of the Jisc member to ensure that they consult with all relevant roles and groups within their organisation, and take their views into consideration as appropriate, before acting upon any of the supplied advice or information.