Responses to Frequently Asked Questions IT/IG:

How do we protect anonymity of individuals whose job titles effectively identify them? (Just to give a couple of examples, Chief Executive, Head of Communications etc.)

We protect privacy by assigning keywords to Job Data, not using the raw data itself.
As an example, if the role of Chief executive was recognised, it would be assigned the keywords or 'directors' and 'senior managers' - This is the information that we would store. As many roles/job titles etc can be mapped to each keyword, it is not possible to map keywords back to a specific role.

How do we deal with the fact that staff are not being able to opt in (since this is for work purposes using work IT)?
Our current basis for processing data is that of legitimate interest - via the commercial relationship between the Trust and Fendix Media.

How do we protect our IT systems in the unlikely event of your server being hacked?
The simplest option is just to switch off the serving switch in the configuration of the trust side component – this disables the entire process. Our servers do not require any inbound access to the trust network, so it is no different to any other website or service.

If, for whatever reason, you have any issues with your ad-server, could it potentially cause issues for our IT system (e.g. causing our intranet to crash or go slow)
We recommend loading ads asynchronously using the third party post-scribe library, which loads ads in the background without delaying the rest of page load – that way in the event of an issue with ad serving (or as has proved much more likely, issue with the N3/HSCN) it does not affect page load.

How can we be sure your pseudonymisation is completely reliable?
We do not transmit any identifiable user details outside of the Trust network, we hash the user's email address using a unique salt for each user and then hash using the SHA512 hashing algorithm. This hash is then also Base64 Encoded and sent over a secure (HTTPS) link to our server.
Hashes are none reversible, so we also hash email addresses using the same system in our copy of the ESR File which is held on our IG Compliant secure server. In order to match a user to Job Role, Occupation and Department, we compare the incoming Hash from the Trust to the Hashes in our ESR Database. Once we have retrieved the Job Role, Occupation and Department, we perform a Keyword lookup to retrieve the keywords used in selecting campaigns, for example, (cardiac) (diabetes) (doctor). Once we have the keywords, we delete the Hash that came in from the Trust, so it is never stored anywhere and only in use within the server memory used by our code.
Given that cracking the hash would be extremely difficult and bring no benefits to an attacker it would be pointless to brute force attack. Hashes are only used during the Banner selection process and then deleted.

If you are collecting information about pages visited or click-throughs in order to report back to clients, what guarantees can you give that you do not share or further process data?
The only information we share with clients is statistical information such as page impressions or click throughs. We do not share personal data of any form (we do not have access to any)– to do so would be a GDPR violation as we do not have opt ins to share personal info with any named third parties.

Can staff opt-out of the ads?
It is not currently possible for individual users to opt out of ads.
With the ESR based segmentation, targeted ads could be disabled on a per individual basis by removing the relevant individual from the ESR data file, they would still see generic run of site ads.

Will it slow down the Intranet?

No. Ads can be loaded asynchronously using an open source script library that is designed specifically for ad loading – this way the ads load in the background without causing the page to wait.

Do you regularly check links and remove links that could be potentially unsafe?

Yes. We only accept campaigns directly from clients and trusted ad agencies that we have a direct relationship with. All campaigns are checked prior to release to the Trust and all campaigns are explicitly approved by the trust prior to delivery.

What's the guarantee of the security of the sites the banner click is going to?

See above - as we work directly with the agency or end client all click through destinations are known. As the destination sites are on the open internet, normal considerations regarding site safety apply. Landing pages are communicated to the Trust as part of the campaign approval process prior to delivery.

We share the list of the sites that need to be whitelisted to your IT teams during the installation phase. we won't just open a site.

Our standard recommended whitelist is at:
https://www.fendixmedia.co.uk/segmentation/FMWhitelist.pdf
This covers the most common domains that ads are linked to by partner agencies. If the trust chooses not to whitelist any of these domains, it may impact eligibility for some campaigns and thus revenue.

What disclaimers are there around content of the sites e.g. The Trust is not liable

The trust can place disclaimer text either above or below the banner. Alternatively, a disclaimer message can be injected along with the banner which allows for an information message to be displayed if the user clicks an icon in the corner of the banner.

What input do you get from would-be advertisers? And what information do you supply to them?

Advertisers are able to select the broad specialism keywords that they wish to target their ads for serving to (e.g. doctor's, procurement, cardiac). They are able to choose these from a pre-defined list. For example, Macmillan Cancer Support recently ran a campaign to inform healthcare professionals of the support information available to patients. They wanted to target this campaign to nurses, cancer and palliative care. The only information that is supplied to advertisers is the number of ad impressions served against the chosen keywords (if they request this level of granularity, typically an advertiser is only given a report of the number of impressions served and the number of clicks generated)

At no point do advertisers have access to actual user roles, nor how they are mapped to specialism keywords. Advertisers are also not advised as to how many roles are mapped to a keyword, nor how many users have a given role.

What trust information is transmitted to Fendix media and how is it used?

The following information is transmitted to the segmentation servers:

- Secure hash of user's email address - this is used to look up the user's role, occupation, and area of work (Department) in our own copy of the ESR file - these are used to allocate keywords for ad targeting. It is not used to track individual users. A secure hash is a nonhuman readable representation of the original email address. In addition, hashing is a one-way mathematical process that cannot be reversed to obtain the original email address. At no point do Fendix Media receive actual usernames.

The segmentation service accepts secure HTTPS requests. This data is only held on our servers and access is not shared with anyone outside of Fendix Media. No trust data is transmitted outside of the Fendix server infrastructure.

Where is this run from - locally or cloud based? Where is your ad server hosted and how secure is it? What precautions do you take to ensure security?

There is a small component that resides locally on the trust network, the rest of the segmentation system is hosted by Fendix Media.

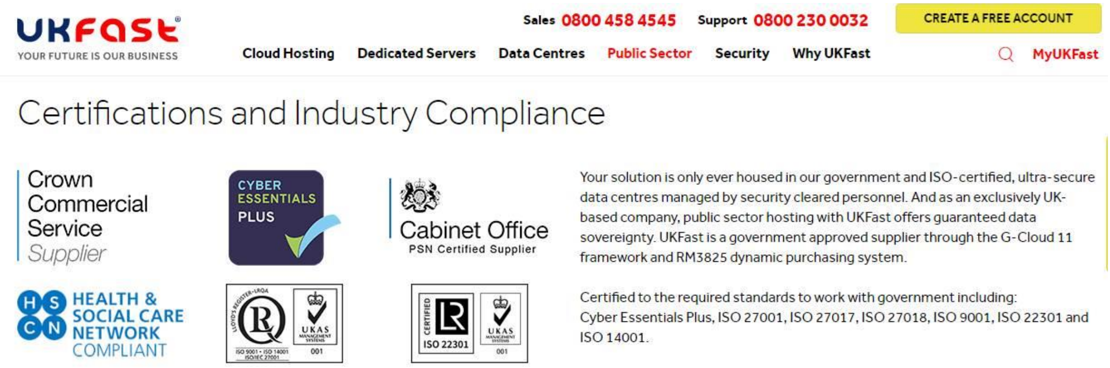
Our Servers are IG Compliant, Cyber Essentials Checked and Penetration tested as part of our ISO 27001 Certification and NHS Digital Data Security and Protection Toolkit Registration.

CHECK IT Health Check Service | CYBER ESSENTIALS | NHS Digital Data Security and Protection Toolkit

All of our servers, including the AdServer are hosted at UKFast in the Government Services hosting centre in Manchester, alongside servers from HMRC, several NHS Trusts, and other Government departments.

The security and patching is provided by UKFast, and is certified secure to the highest standards.

We cannot even physically access the servers ourselves, and our own access is via a secure jump server portal.



Certifications and Industry Compliance

Crown Commercial Service Supplier

CYBER ESSENTIALS PLUS

Cabinet Office PSN Certified Supplier

HEALTH & SOCIAL CARE NETWORK COMPLIANT

LLOYD'S REGISTER LRQA ISO 9001 • ISO 14001 ISO/IEC 27001 UKAS MANAGEMENT SYSTEMS 001

CERTIFIED LR ISO 22301 UKAS MANAGEMENT SYSTEMS 001

Your solution is only ever housed in our government and ISO-certified, ultra-secure data centres managed by security cleared personnel. And as an exclusively UK-based company, public sector hosting with UKFast offers guaranteed data sovereignty. UKFast is a government approved supplier through the G-Cloud 11 framework and RM3825 dynamic purchasing system.

Certified to the required standards to work with government including: Cyber Essentials Plus, ISO 27001, ISO 27017, ISO 27018, ISO 9001, ISO 22301 and ISO 14001.

We do not allow any client to place ads directly into our system. We only accept ads from trusted partners who we have a relationship with, and we put the banners into our system ourselves.
Any banners are thoroughly checked by us for malware, and content, and the sites will be required to be whitelisted by the trust, thus forming part of a closed loop trusted network.
Access to the internet at large is controlled by the trusts normal firewall security mechanisms and there should be no possibility of malware entering your network.