

e-KSF and your data

This document describes what data e-KSF stores about individuals, and how this data is processed and displayed to other people.

The e-KSF is a secure online database. There is a large store of electronic information behind the web pages that you see when you record reviews and personal development plans. This electronic information is used in the set-up and maintenance of e-KSF for your organisation, and is also displayed as people use the e-KSF system. The remainder of this document describes in more detail how this data is collected, used and displayed.

What data does e-KSF store?

As your organisation uses e-KSF, the following information will be collected:

- Basic information about your employment, for example your name, pay band, pay increment date and pay point (but not your specific salary)
- Information about where you work
- Information about your work-based phone numbers and emails
- Information about the KSF Post Outline/s for your job
- Information about how you and your reviewer view your progress against the Knowledge and Skills Framework
- Information about your Personal Development Plan.

Please also see the section "[logging on for the first time](#)" for an explanation of how we record your agreement to the e-KSF terms of use. You can see a full list of the personal data held about you on e-KSF, by logging in and clicking the "View Personal Details" button

We do not store any form of hidden data - the only information we hold about you and your job is the information that you, your manager or your organisation's e-KSF administrator enter onto the system.

We use the information we collect in the following ways:

- To present to you, and your manager, an analysis of how you're doing against your KSF post outline, and also to allow you to create and store a personal development plan on-line
- To respond to questions you send us about using e-KSF.
- To create aggregated reports on how many people are using this system, and what sort of data they are entering. These reports do not identify any individual. They only give overall numbers, for example, of the number of people who have had a review in your organisation, or the number of people who have updated their personal development plan. They cannot be used to identify who has done this. These reports will also be used for equality monitoring – for example, to check that everyone has an annual development review irrespective of position in the organisation

You can be assured that:

- Your data is kept safe on a set of dedicated computers, protected by secure encryption and firewalls (which means that measures are in place to minimise the risk of anyone "listening in" on data as it's transferred from your computer to our server, and of

anyone electronically “breaking into” our servers). See the [“how is data kept secure”](#) section of this document for a more detailed explanation of this.

- Once you leave the NHS your data will no longer be identifiable, although we may keep it in anonymous form for benchmarking purposes. For example, the NHS may want to see how use of the e-KSF changes over the years, and the fact that, say, 200,000 people used e-KSF in 2005 would be useful for this. Of course, individual staff can never be identified from this benchmarking data.
- We will never provide your data to any other organisations or individuals unless required to do so by the data controller under any applicable law (please see the section on [“who runs the e-KSF”](#) about which organisations can currently access data).
- We will never sell, lease or give your data to anyone without authority.

How does basic data get put onto e-KSF?

Before you log in to e-KSF, the system needs to know a little bit about you. This is to ensure that you see only the information that you are allowed to see and the screens that are relevant to you (i.e. you can see your own Personal Development Plan on-screen, but not your colleague’s plan). This basic data also helps organisations to maintain e-KSF and run equality-monitoring reports to check that no-one is disadvantaged as the KSF is implemented.

The exact method of getting this basic data onto e-KSF will vary depending on decisions made by your organisation, but there are two basic ways of doing this.

- 1) Users register basic details themselves. You may be asked by your organisation to register yourself on e-KSF by entering your name and other details. In this instance, e-KSF needs some very basic information – first and last names, employing organisation and some unique way of identifying you, e.g. your payroll number. Your organisation will tell you what unique identifier you need to use. (see also the section of this document: [“why do you need payroll numbers or National Insurance numbers?”](#)). Your employers might ask you to enter other information (for example your job title and contact telephone number) but they should explain the reasons why they want you to do this.
- 2) The administrators of e-KSF in your organisation register the basic details of all staff in the organisation. Your employers may decide that it’s more efficient to add basic data to e-KSF via spreadsheets or links to existing HR systems like ESR (England and Wales) or SWISS (Scotland). In this instance, the organisation may upload a range of information on your behalf, for example name, unique identifier, department, job title etc. The more information that is uploaded to e-KSF, the more comprehensive the reporting capabilities meaning that it’s easier for the organisation to monitor the roll-out of e-KSF (however, your personal data is kept secure – see the [“who can see the data”](#) section of this document). Your organisation should decide what is added to e-KSF, in partnership with staff-side representatives.

Once this basic data is added to e-KSF – by the named administrator(s) in your organisation – the only other personally-identifiable data that gets added to e-KSF is entered by you or the person who is your reviewer in relation to the KSF.

Logging on to e-KSF for the first time

When you first log on to e-KSF, you’ll be asked to accept a terms and conditions page (which includes a summary of the information in this document). In common with most websites, you can only use e-KSF by agreeing to these terms and conditions. If you have any difficulties or questions around these terms and conditions, you should in the first instance discuss it with

the relevant person in your organisation (e.g. KSF management lead, staff-side lead or data protection officer).

Why do you need payroll numbers or National Insurance numbers?

The e-KSF system needs some unique way of identifying staff with the same or similar names – across the whole of the NHS, not just in one organisation. For example, if there are two employees called Tim Newham in the NHS, then e-KSF needs some way of identifying which post outline, review and PDP belongs to which person.

There are two main choices for this unique identifier. The Payroll or Employee number held in HR systems can be used (but this may not be unique across the whole NHS so we need to store it in combination with organisational data) or your National Insurance number, which is unique to every individual in the UK.

These identification numbers are only ever seen on the system by the individuals concerned and their e-KSF administrator.

We will also need to use these unique identifiers in the future. With the implementation national payroll systems (such as the Electronic Staff Record (ESR) in England and Wales), it may also be necessary to match up records between e-KSF and these payroll systems, and National Insurance numbers are often the most accurate way of providing this link, so using NI numbers as e-KSF identifiers makes technical sense.

Some organisations have already chosen to submit NI numbers as bulk uploads to the e-KSF team, and these are used purely for data identification purposes maintaining strict confidentiality. The use of National Insurance numbers in e-KSF has been approved by the national “NINO Board” – a cross-departmental government committee which oversees the use of National Insurance numbers. You can read more about the NINO board here:

<http://www.hmrc.gov.uk/manuals/nimmanual/NIM39710.htm>

I’ve heard that e-KSF stores personal data like gender and ethnicity. Why is this?

The NHS will need to check that the KSF is being implemented fairly across all groups. In order to do this, the reports from e-KSF will need to be able to identify gender and ethnicity groups to ensure that all groups are being treated equitably. Your gender and ethnicity data, and other demographic data that may be required in future reports (e.g. age, length of service) will ONLY be used to check fairness of implementation of the KSF across different groups and to ensure compliance with Equal Opportunities legislation. It will not be used for any other purpose, and no reports available to the NHS will link this data to individual employees.

Who can see the data added to e-KSF?

Within your organisation

e-KSF has security and confidentiality built in. Because people within organisations have to use web pages to access data stored in e-KSF, we can be sure of who can see what by carefully designing these web pages to only display relevant data to each user. E-KSF is designed so that:

- ONLY an individual and their direct reviewer can view the detail of that individual's development review and PDP. Your personal data will not be disclosed to any third party organisations, including NHS organisations, other than as required by the data controllers under any applicable law.
- Aggregated reports will be available to administrator-level users in your organisation. These reports may also be shared with other people in your organisation – for example HR and training departments who would be interested in how departments and divisions are doing against the KSF. **However individual staff can never be identified from this aggregated data.**

Within the NHS generally

Other NHS organisations, for example Strategic Health Authorities/ Health Boards, will also run reports from e-KSF to check how the KSF is being implemented. Once again, NO personally-identifiable data will appear in these reports. These reports will just be aggregated pictures of how the KSF is being used across whole organisations and/or staff groups.

Outside the NHS

The e-KSF is maintained by two private organisations – Think Associates Ltd and Ikonami Ltd. The e-KSF account managers, project managers and support desk staff are employed by these organisations. Please see the next “who runs e-KSF?” section of this document for more about these organisations, and the limits on how staff in these organisations can use e-KSF data.

Who runs e-KSF?

The e-KSF system is being developed and maintained by a private organisation called Think Associates Ltd. Think Associates is a Human Resources and Change Management consultancy. Think Associates is subcontracted by the Department of Health and Tim Newham, a Director of Think Associates, attends the UK KSF policy group (KSFG).

The e-KSF “super-administrator” functions are jointly run by Think Associates, Ikonami and the KSFG.

The e-KSF is overseen by the KSF Group of the NHS Staff Council, and decisions about what data to store, use and display via e-KSF are taken in partnership with NHS employers and staff-side or representatives. Because of this process, you can be sure that the views of all stakeholders are taken account of when managing the Think Associates and the e-KSF project.

Employees of Think Associates are subject to strict data protection policies. Although employees do need to view e-KSF data in order to do their jobs, they can ONLY use this data in order to complete their specific tasks, and can NOT share this data with anyone outside the organisation.

Think Associates Ltd is registered with the Data Protection Agency, registration number Z8829404.

Think Associates subcontracts the technical development, build and some of the support of e-KSF to a company called Ikonami Ltd. Ikonami is a specialist IT company. Ikonami is subject to the same strict data confidentiality and security management policies that Think Associates has signed up to. Ikonami's Data Protection registration is PZ8885598.

Think Associates and Ikonami Limited operate the e-KSF and act as data processors in relation to the personal data, acting on the instructions of the relevant National Health Service employing organisations. The data controller of the personal data is the organisation employing the individuals whose data is contained in the e-KSF. Any queries about data, or corrections to personal data, should in the first instance be directed to your local organisation's e-KSF administrator, KSF lead or HR department.

Where is the actual e-KSF data stored?

Think Associates leases a set of computers in Bristol, UK, which store the entire e-KSF database. This database is backed up daily and kept off-site in Bristol. No other copies of the data are stored anywhere. The e-KSF support desk dealing with personal queries is based in the UK, so even though some of the e-KSF technical support and IT programming teams are based outside of the UK, no personal data is transferred outside of the UK.

How is data kept secure?

As e-KSF is accessed via the internet, we've taken special precautions to ensure that users' information is kept secure. To do this, we have three stages to our security.

- Firstly, the data that people submit to the tool is kept physically under lock-and-key at our servers in Bristol, which is also protected by a "firewall" meaning that it is secure against electronic attack.
- Secondly, data in transit over the internet is encrypted (encoded) using "secure sockets layer", which means that anyone "eavesdropping" on the data will not be able to make sense of it.
- Thirdly, information on users' computers is only displayed once a password, only known to the individual user, is entered. This password also ensures that registered users only see the data that they should (so, for example, information about an individual's personal development plan can only be displayed to that individual and their reviewer). This emphasises that you need to keep your password safe and secure, and change it if you suspect anyone else knows what it is.

I'm from an IT department – what else should I know about e-KSF security policies?

For the more technically minded, we've listed a few other procedures which are in place to ensure security on the e-KSF tool.

Our tool is running on HTTPS which ensures secure, encrypted communication (between the client machine and the server) thereby practically eliminating any chance of data being intercepted on the way.

Other ways to "break into" a website include SQL injection, trying to put foreign code into system through systems input boxes especially on search pages. Our application architecture makes this impossible, through the use of application tier, data tier and DB Stored Procedures.

Another risk for information to be leaked is through caches maintained on client machines and proxy servers. We have enabled an option in our pages whereby our pages are not cached on any proxy server or client machines. Currently this has been done on most of the pages of the application excluding popup pages, because of time constraints given the number of popup pages we have (though this is being implemented as we speak/type/read).

We are also using “Forms Authentication Security Measure” on our site to make sure that there is no un-authorized access to any resource, which eliminates any chance of anyone accessing data without going through the e-KSF login page.

When we need to link e-KSF to other systems (like payroll systems), these links are implemented using standard technologies like SOAP and XML which are Industry Standard. The data structures displayed to other systems for integration are always different from what they are within the e-KSF system itself, so no-one could work out the internal structure of the e-KSF database.

Web service security in the IT industry is evolving all the time, and being registered with MSDN (Microsoft Developers Network) we are kept up to date on all new releases from Microsoft, meaning we stay on top of emerging matters.

We have a range of detailed technical security measures in place. However, please bear in mind that complete details of the security measures described above can not be released, since these are themselves under lock and key!

What do I do if I have more questions?

If you have any other questions about data security and confidentiality, please in the first instance contact your local e-KSF administrator or KSF lead. If you need further clarification, please contact the KSF Group of the NHS Staff Council via agendaforchange@nhsemployers.org.

*Tim Newham
e-KSF Project Manager, and Director of Think Associates Ltd
First draft: 20th January 2006
Document updated: 31st March 2008*