

# For the supply of DfE Data Extracts – Information Security Questionnaire

Please complete this form if you require a DfE data extract delivered direct to your organisation.

# DfE Use only

|  |  |
| --- | --- |
| **Internal Reference** |  |
| **DSAP Number** |  |
| **Date scored (DD/MM/YYYY)** |  |
| **Total score** |  |

# SECTION 1 – Contact Details

Name of Applicant

|  |
| --- |
|  |

Name of person / organisation who will be entering into the Data Sharing Agreement (“the Requester” / “the Recipient”)

|  |
| --- |
|  |

Name of Responsible Individual (if different from above)

|  |
| --- |
|  |

Email Address (must not be a personal address)

|  |
| --- |
|  |

Telephone number

|  |
| --- |
|  |

Name of person to whom the data will be transferred to

|  |
| --- |
|  |

Name of organisation’s IT Security Officer

|  |
| --- |
|  |

Email address

|  |
| --- |
|  |

Telephone number

|  |
| --- |
|  |

# SECTION 2 – Questionnaire

**Please answer all questions below.**

## Information Security Policy

**1. Does your organisation have an up-to-date information security policy, which will be adhered to, in relation to handling DfE data? Please provide a copy.**

Your evidence should be able to demonstrate that your security policy is both in place and enforced and this should be accompanied by a statement of support from a senior manager.

Organisations that are unable to provide a sufficient information security policy should provide a statement of support from senior management. This statement should describe the measures taken to ensure data will be secure.

|  |
| --- |
|  |

**2. Are you certified to ISO27001, and does the scope of this certification cover all areas of your arrangements for handling DfE data?**

**Alternatively, if you are not ISO27001 certified, does your information security policy align with this standard and, if so, how is this alignment achieved?**

**ISO27001 certified**

Please provide either a certificate reference or a copy of the certificate. Indicate the full scope of the certification and explanation of any exceptions in your Statement of Applicability that are relevant to your arrangements for handling DfE data.

**ISO-27001 aligned or not**

Please provide evidence to show how the alignment of the security policy has been achieved and its relevance to your arrangements for handling DfE data.

|  |
| --- |
|  |

## Technical System Description

**3. Give details of the type of network system and application you will use to process DfE data. In particular, specify whether the system is stand-alone, attached to a corporate network or connected to the Internet**.

Your answer should describe the technical environment within which data sourced from the department shall be hosted. This description should include details of any hardware shared with other parts of your organisation e.g. a shared storage device or database.

|  |
| --- |
|  |

**4. Confirm the system is running currently supported versions of operating system and other software and that these are regularly patched as required.**

Your response should be sufficient to indicate that the software you are using to host DfE data is not obsolete (out of vendor support) or subject to unpatched security vulnerabilities.

Indicate how the patching regime works for your devices' operating systems and key software that will process DfE data. Is this an automatic or a manual process?

|  |
| --- |
|  |

**5. Will the computer system hosting DfE information be accessible to remote users, such as via a dial-up modem or remote access over the Internet?**

**If yes, please describe the requirement for remote access and whether any encryption over the link is in place (e.g. VPN, SSL/TLS). Indicate how remote users are authenticated to your system.**

Your response should:

* Describe any encryption algorithms used and associated key lengths for encryption of data in transit (e.g. VPN, SSL/TLS) and at rest on remote devices e.g. hard disk encryption.

● Describe the user authentication mechanisms used at a high level e.g. password, token-based or certificate-based.

* Indicate controls in place to prevent or secure the downloading of DfE data to the remote devices (e.g. hard disk encryption, USB port control, any physical / personnel controls).

|  |
| --- |
|  |

**6. Confirm that appropriate security access and/or firewall controls are implemented on:**

**● The system hosting DfE data.**

**● Any LAN, WAN or Broadband / ADSL router to which it is connected (whether physically or wirelessly).**

Your answer should describe the implementation of the safeguards below, specifically:

- Name the anti-virus products used and how new virus signatures are distributed.

- Name the firewall products used.

- Describe the user authentication mechanisms or gateway (e.g. email) controls in place.

|  |
| --- |
|  |

**7. Can you confirm (and provide evidence) that copies / backups of DfE data will be subject to the same security standards as the systems holding the live data?**

Answer Yes or No.

Your evidence should refer to named policies in place and the encryption methods used for copies / backups.

|  |
| --- |
|  |

## Physical Security

**8. Describe the physical security arrangements for the location where the information is to be:**

**● Processed**

**● Stored (if these are different)**

Your answer should describe how you prevent those who are not listed in this request as accessing the DfE data from doing so. Examples include the use of separate locked rooms for analysis of DfE data, locking away media containing the data etc.

If you are processing DfE data in an environment with layered physical security (e.g. a secure perimeter, CCTV, security guarding or a locked room) or in a container such as a locked cabinet, then please describe this environment.

If you are storing DfE data on a PC or laptop that is not located in an environment with layered physical security then please specify what type of hard-disk encryption you use and whether this product is FIPS 140-2 certified.

|  |
| --- |
|  |

## Data Handling

**9. Where do you plan to store and/or process the data that we may provide?**

**● UK mainland with no IT connection to public networks (e.g. Internet).**

**● UK mainland, but with accredited IT connection (e.g. GSI, JANET) to a public network.**

**● UK mainland, but with non-accredited IT connection to a public network (e.g. Internet).**

**● Accredited overseas offshore solution.**

**● Overseas (including online services where our data is not guaranteed):**

**a. EEA**

**b. US**

**c. Elsewhere**

**d. Don’t know**

In answering the question please provide details of the actual site / location.

As a rule, departmental policy does not allow for processing of data overseas but this may be permitted in exceptional circumstances. Requests to process the most sensitive data overseas must be cleared in advance by the department with the Office of the Government Senior Information Risk Owner (OGSIRO).

|  |
| --- |
|  |

9a. Please provide details of the measures you are putting in place if you are considering to share DfE data with any countries not on [UK’s adequacy list](https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation#uk-adequacy). State the country you intend to share with. See ICO website for further information on [international transfers](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#Q1) of personal data.

|  |
| --- |
|  |

**10.What policies do you have in place:**

**● Dictating when DfE data and or information can or cannot be printed in hard copy or written to removable media?**

**● Covering the handling and control of any hard copy and/or removable media containing DfE data?**

**● Dictating when DfE data and or information can or cannot be transmitted electronically e.g. e-mail?**

Your evidence should refer to named policies (including links to the appropriate section in the policy) and note any encryption standards e.g. FIPS 140-2 or AES-256.

|  |
| --- |
|  |

**11. Confirm that DfE data will be encrypted if:**

**- Electronically transmitted, copied, or transferred outside your secure environment in its raw form or across an unsecured network.**

**- Stored on a standalone PC in an environment without layered physical security.**

Your response must confirm that encryption will always be used in these circumstances. You must provide details of the tools to be used and the encryption standards they meet (and, in particular, whether they are either validated to FIPS 140-2 or, as a minimum, implement AES-256 encryption).

This requirement to encrypt data applies to any electronic transfer including e-mail, file transfer and saving onto removable media such as USB sticks, writable CD / DVD, or portable hard disks (including laptop disks).

If you do not plan to transfer the DfE data your evidence should still list the available encryption standards.

|  |
| --- |
|  |

## Staff Awareness

**12. Does everybody in your organisation handling data know and understand when they can / cannot share information with other members of staff?**

Your evidence should refer to where this guidance is documented.

Confirm whether or not there is clear guidance highlighting that deliberate or accidental compromise of personal data may lead to disciplinary action and/or criminal proceedings?

|  |
| --- |
|  |

## Risk Assessment

**13. Do you have documented control measures in place to regularly review the people, processes and technology risks that may impact upon your arrangements for secure handling of DfE data?**

Your evidence should:

• Indicate whether your organisation has carried out a review in the last 12 months.

• Confirm when your last review took place.

• Confirm whether all or some of the requirements for remedial action have been satisfied in a timely manner.

If your process includes any element of periodic independent review then please indicate this in your response

|  |
| --- |
|  |

## Audit and Monitoring

**14. Are there arrangements in place to routinely monitor and audit access to the computer system and address any potential misuse / abuse or breaches of the agreed information security controls?**

Answer Yes or No.

If Yes, your evidence should be able to show that either documented procedures (please provide a copy) or effective logging and audit mechanisms are in place with regard to access to DfE data.

If No, indicate how you would know if a non-authorised person gained access to the data and/or what controls you have in place that would prevent access by such people. Indicate what you would do in the event of a security breach.

|  |
| --- |
|  |

**15. What are the System internal / external audit arrangements?**

Your response should describe whether the system is subject to internal and/or external audits and by whom such audits have been conducted. Your response should also indicate when the last audit was conducted and to what extent the audit findings have been satisfactorily addressed.

|  |
| --- |
|  |

**16. Have you had any security / data breaches in the last 12 months?**

Your response should describe each breach, how you handled it, how you informed the ICO (if relevant) and the data subjects (if relevant). Your response should also state what changes you have made to policies, procedures to mitigate the risk of another breach occurring.

|  |
| --- |
|  |

## Sanitisation and Disposal

**17. Describe the method of data destruction you will employ when you have completed your work using the DfE data.**

Data should be deleted so it ceases to be copied to backups, and secure file deletion software should be used so that unerase / undelete utilities cannot recover the data. All media on which DfE data has been processed should be shredded, destroyed using commercial best practice, de-magnetised, or securely erased. Any paper copies should be cross-cut shredded, pulped, or incinerated. Describe the processes for controlling the re-use of ICT equipment including (where necessary) the secure deletion of DfE data?

Provide details of documented procedures in place and the tools used (including name of secure deletion product) for the controlled disposal i.e., secure destruction, overwriting, erasure or degaussing of electronic media used to store DfE data on completion of your work.

If you are claiming an exemption under Data Protection legislation which allows you to retain DfE data indefinitely then provide details of the exemption and why it is applicable to your situation.

If your organisation does not have a documented procedure, then please describe your processes for ensuring that DfE data will not remain on storage devices that will no longer be used for DfE data.

|  |
| --- |
|  |

**17a. In line with ICO guidance on erasing data from backups and deleting personal data, describe how you would put DfE data “beyond use”.**

Data should be deleted in such a way that it ceases to exist in backups or is put “beyond use”.

Provide details of documented procedures in place and any tools used for the controlled disposal of DfE data from backups.

If your organisation does not have a documented procedure, then please describe your processes.

|  |
| --- |
|  |

**18. If not securely destroying storage media holding DfE data, name the product that you will be using to securely erase the media prior to it leaving your premises.**

A simple "delete", for example, by sending a file to the Windows Recycle bin and then emptying the Recycle bin, does not actually remove the sensitive information from the file system. Secure erasure products will overwrite the information on the file system (usually multiple times) which makes it much harder for an individual to then retrieve the information from the hard disk without access to highly specialised equipment.

Your response should name a product capable of providing secure erasure capabilities through multiple overwrites and state the number of overwrite cycles used.

|  |
| --- |
|  |

## Third Party Access

**19. If information sharing is expected, provide a full description of the relationship between yourself and the relevant third parties and the proposed arrangements and security measures imposed upon the relevant organisation(s).**

Your evidence should explain:

● Why the information sharing is necessary.

● Why the third party has not approached the Department for Education directly for access to the data.

● How you will ensure that information sourced from the department shall be secured whilst in transit to the third party.

● How you will ensure that information sourced from the department shall be secured whilst in the custody of the third party.

● How you will ensure that information sourced from the department is only used for the purposes specified in this request.

|  |
| --- |
|  |

**20. Do you have any agents such as sub-contractors or suppliers who are not directly employed by your organisation who assist in the delivery or support of your product or service who may access our data? For example, is management of your ICT systems outsourced to a third party?**

Answer Yes or No.

Your response should also list such suppliers and the nature of their involvement in your handling of DfE data.

|  |
| --- |
|  |

**21. Does your organisation have effective and accurate mechanisms in place to monitor the status of the control measures employed by your sub-contractors?**

Answer Yes or No.

If Yes, your evidence should be able to demonstrate that processes for monitoring sub-contractors control measures are in place.

|  |
| --- |
|  |

# SECTION 3 – Signatures

To be signed by the organisation that will be receiving a direct supply of DfE personal data.

|  |  |
| --- | --- |
| **Name of organisation** |  |
| **Name of signatory** |  |
| **Role of signatory** |  |
| **Signature** |  |
| **Date (DD/MM/YYYY)** |  |

# DfE Use only

|  |  |  |
| --- | --- | --- |
| **Question** | Score | Comments |
| **1** |  |  |
| **2** |  |  |
| **3** |  |  |
| **4** |  |  |
| **5** |  |  |
| **6** |  |  |
| **7** |  |  |
| **8** |  |  |
| **9** |  |  |
| **9a** | N/A |  |
| **10** |  |  |
| **11** |  |  |
| **12** |  |  |
| **13** |  |  |
| **14** |  |  |
| **15** |  |  |
| **16** |  |  |
| **17** |  |  |
| **17a** |  |  |
| **18** |  |  |
| **19** |  |  |
| **20** |  |  |
| **21** |  |  |
| **TOTAL** |  |  |
| **Pass/Fail** |  |  |

**© Crown copyright 2023**

You may re-use this document / publication (not including logos) free of charge in any format or medium, under the terms of the [Open Government Licence v3.0](http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this document should be sent to us at data.SHARING@education.gov.uk