|  |
| --- |
| Wibsey Web Logo |

**WIBSEY PRIMARY SCHOOL**

|  |
| --- |
| **DATA HANDLING POLICY** |

|  |  |  |
| --- | --- | --- |
| Agreed by Governors  Date: | Full Governors | ✓ |
| Finance and General Purposes |  |
| Teaching and Learning |  |
| Signed on behalf of Governing Body by Chair of Committee: |  |  |
| Approved | October 2018 |  |
| Review | October 2021 |  |

**Contents**

[1. General Principles 3](#_Toc489859710)

[2. Transfer of Data to a Third Party Data Processor 4](#_Toc489859711)

[3. Sending Personal or Sensitive Personal Information Externally 5](#_Toc489859712)

[4. Confidentiality 5](#_Toc489859715)

**1. General Principles**

**1.1** In order to remain compliant with the Data Protection Act 1998 (the Act) those handling data on behalf of Wibsey Primary School are expected to:

* + Stop and consider whether they should be accessing or disclosing personal data before they do so.
  + Be aware that according to Data Protection Act, they may be personally liable for any data disclosure.
  + Individuals handling Wibsey Primary School data must make sure that they have appropriately verified that the person they are passing data on to, is who they say they are and are authorised to receive it. To do this, the identity verification processes should be used. However, individuals should be aware that by doing so, they are taking personal responsibility for this and may be required to justify their action in the event of a complaint.
  + Not discuss information about colleagues and other stakeholders with unauthorised colleagues, family or friends, or other Wibsey Primary School staff or associates.
  + Not access Wibsey Primary School records containing personal data other than for a specific business purpose. This may also be an offence under the DPA and they may be prosecuted by the Information Commissioner’s Office. This may also result in disciplinary action.
  + Avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes, unless they have given written permission for it to be used.
  + Not express unsubstantiated personal opinions in file notes or e-mails. Individuals may have a right to see the information and may exercise that right.
  + Use the blind carbon copy (BCC) option when sending out the same e-mails to others unless recipients have agreed to share their personal email addresses with others on the list.
  + Consult the line manager and if necessary the Data Protection Officer before starting any projects involving the processing of personal data.
  + Always consider data security and the risks associated with losing personal data, before downloading/printing any personal data.
  + Never share a computer password or write it down. Doing so could result in unauthorised access of personal data and, therefore, could constitute a serious security breach.
  + Ensure their passwords are created in line with the IT Security policy.
  + Always secure devices when leaving unattended – even if it’s only for a few minutes. Always remember to log off devices or services at the end of the day or when no longer required.
  + Take adequate precautions to protect Wibsey Primary School data in a public place; this includes use of mobile phones, laptops/iPads.
  + Be aware that if adequate precautions are not taken by individuals, they are personally accepting the risk of working in this way and the consequences if personal data is left insecure, lost or if there is a complaint.
  + Do not to leave documents containing personal data in or on a printer, photocopier or scanner. Fax machines (considered outdated and insecure by the ICO) should not be used to transmit personal data.
  + Make sure that personal data cannot be seen or accessed by unauthorised individuals; paper based documents should be stored securely in a lockable cabinet when no longer required.
  + If sensitive data is taken out of a building, it needs to be stored in a locked bag or a bag with a padlock.
  + When travelling by car, papers must always be transported in a secure part of the car out of sight i.e. in the boot of the car. Papers must not be left in the car overnight; when at home keep them in a locked bag or secured cabinet.
  + Dispose of confidential waste and paper copies containing personal data in confidential waste bins or by shredding using a cross cut shredder should be used in all cases).In case of large volumes of confidential waste for homeworkers, contact a line manager or Data Protection Officer to ascertain a secure disposal option.
  + Encrypt personal data using the Guidance on How to Encrypt a Document.
  + Data must only be extracted from the database with prior approval of the line manager and the control of the data whilst extracted is the joint responsibility of the “data extractor” and their manager.
  + Those needing to extract more than 1,000 personal data records or 10 sensitive personal data records for Wibsey Primary School processing are to seek the written approval of their manager or Data Protection Officer before proceeding.
  + Take **immediate** action in the event of a Data Breach to prevent any further breaches and report any breach to the Data Protection Officer and relevant Director .

**2. Transfer of Data to a Third Party Data Processor**

**2.1** Before personal data is transferred to a third party data processor, a formal written Data Processing Agreement should be in place between Wibsey Primary School and the data processor. This agreement should clearly state the data processors obligation to treat the data in accordance with the provisions of the DPA, the reasons for the transfer, the time period, what it is required for, how it will be processed and what actions will be taken to delete data when no longer needed.

* 1. Data Processing Agreements are initiated and managed by Wibsey Primary School Data Protection Officer and employees should ensure that they have checked with the Data Protection Officer that a signed Agreement is in place before organising a transfer of personal data to a third party. Note that the Agreement is only valid for the data transfer within the EEA and anything else is not permissible (unless special arrangements are made).
  2. Once an agreement is in place, data that is to be transferred should be secured. Reasonable precautions should be taken to protect data during the transfer i.e. encryption No electronic or hard copy data files such as case files should be sent through the open post – a secure courier service or special delivery service (includes end to end tracking and signature on delivery) must always be used. The recipient should be clearly stated and the party requesting the information should fund the costs.
  3. If data is sent via a courier or special delivery, the intended recipient must be advised when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

1. **Sending Personal or Sensitive Personal Information Externally**

**3.1** Through its Customer Relationship Management (CRM) platform (database), Wibsey Primary School processes personal information daily to assist and support its employees. The DPA requires that all departments have appropriate security in place to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage. The Data Protection Officer is responsible for identifying and adopting appropriate security measures to protect person information stored on the CRM and other data repositories.

**3.2** If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

1. **Confidentiality**

**4.1** The following principles should be followed wherever sensitive personal information is communicated:

* The purpose for sharing the information is justified.
* Information that personally identifies individuals is not used unless necessary.
* Information is only disclosed on a “need to know‟ basis.
* If unsure then seek guidance on appropriate action from the Data Protection Officer.

**4.2 Face to Face –** Personal information should not be shared in front of others. Employees should ensure that they are not disclosing or requesting the disclosure of sensitive information about themselves or others in front of others, e.g. in reception areas or in a format, that could be viewed by others.

**4.3 Telephone –** Personal information should only be disclosed over the telephone to a third-party where the following procedure has been adhered to:

* The identity of the other party has been confirmed by verification. The type of verification will differ by service and the sensitivity of the information being disclosed.
* The reason for requesting the information has been established and is appropriate.
* Where appropriate, contact details have been requested and their identity checked by calling the person back via the main switchboard of the organisation that they represent and asking for the person by name.
* Provide personal information only to the person who requested it.
* Do not leave any confidential information on voicemail or answering machines as it may be accessible by others. Please remember that by confirming an individual is a member of Wibsey Primary School you may be releasing sensitive personal information as defined by the DPA.
* When in conversation take precautions to ensure that information is not shared inappropriately with others, e.g. when using mobile phones, travelling on trains, etc.
* Sensitive personal information should not be sent via text messaging as it may be accessible by others.

**4.4 Email –** Email services should be used as follows:

* Sensitive personal data (or bulk records) must be encrypted if sent via email. There is no need to use encryption when sending an email containing non-sensitive personal data about less than 10 data subjects, unless the data subject themselves insists on all communication being encrypted. Nevertheless, all need to pay attention to detail to ensure that the recipient’s email address is spelt correctly to ensure this is delivered to the appropriate person. A test email should always be sent before sending sensitive (or bulk) data for the first time. Bulk data information should not be separated into smaller ‘chunks’ to avoid the requirement for encryption.
* Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.
* If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.
* Consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email.
* Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual employee’s records.
* When transferring data, be aware of who has permission to view your emails or who might be able to view your recipient’s inbox.
* When an email does not contain sensitive information relating to a single individual, it does not need to be encrypted.

**4.5 Paper –** Paper files should be managed as follows:

* A clear desk policy should be observed, wherever possible, at all times. At the end of each day no documents containing personal should be left on a desk.
* All files containing personal data should be held in locked filing cabinets, cupboards or draws. Where the data is sensitive it must be held securely at all times.
* Sensitive documents taken into the public domain must be transported in a locked bag.
* A tracer card system should be used when removing a file from the office. The card, inserted in place of the file, should identify the file removed, the holder of the file and the expected return date.

Signed on behalf of Wibsey Primary School: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed by Employee/Associate/Contractor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_