Data Protection Do’s and Don’ts for Staff

The school collects and uses personal information about staff, governors, volunteers, pupils and parents in order to provide education to pupils, employment contracts to staff and meet its statutory obligations as a school.

The school must manage this information in line with the principles set out in the General Data Protection Regulation (2018) and deliver the Individual Rights of data subjects (people). These requirements are detailed in the school’s suite of GDPR policies and procedures. Subsequently this document should be read in conjunction with the following documents:

* **Data Protection and Information Security Policy**

This policy sets out the different types of data that is processed at the school and outlines how that data is processed and kept secure.

* **Privacy Notice for Pupils / Parents; Privacy Notice for Staff/ Governors/ Volunteers**

These documents tell pupils and staff what data is collected, why it is collected, who it is shared with and the legal basis for processing their personal data.

* **Retention Schedule**

This document identifies the different processing activities undertaken by the school and how long the data is retained. In some cases data is archived, which means it is no longer being processed, but it is kept securely in the event of a future request.

* **Record of Processing Activity (ROPA)**

This document identifies the individual data processing activities, the categories of data being processed, the purpose of the processing and who the data is shared with. Any new processing activity must be checked for compliance and then recorded on the ROPA.

* **Data Protection Impact Assessment (DPIA)**

This document is used to review if a new technology or data processing activity meets the requirements of GDPR. The DPO will help produce this document when there is a high level of risk to the security and processing of the data.

* **Individual Rights Request Form**

This document gathers and monitors a request from a data subject for their personal data. It can also be used to meet the additional rights such as amending, restricting or erasing data.

* **Breach Management Form**

This document gathers the details of a data breach. This is where personal data is either lost or accessed by an unauthorised 3rd party. It is very important that any breach is identified as quickly as possible so that the appropriate action can be taken to reduce the risk to the individual and the school.

The following tables give an overview of some of the things that office staff and teachers must do to meet the regulations and some of the things that should be avoided.

**RESPONSIBILITY OF ALL STAFF**

|  |  |  |
| --- | --- | --- |
| **Activity** | **Do** | **Don’t** |
| Gathering of personal data | -Only collect the data you need for the activity and only use it for the purpose for which it was collected. | -Collect anything you don’t have a legal basis to process. |
| Data security (Electronic and hard copy personal data) | -Keep personal data secure using passwords and locked cabinets.  -Ensure data cannot be accessed by unauthorised staff / pupils.  -Ensure the security of any data that is removed from the school. | -Share passwords or leave computers unattended whist processing personal data.  -Leave cabinets unlocked or leave keys accessible.  -Leave personal data vulnerable to unauthorised access.  -Leave personal data on a personal device. |
| Processing personal data | -Take care when processing data, particularly sensitive or special data. | -Assume others will keep the data safe. |
| Disclosure | -Keep personal information within the school as far as possible. | -Share personal data with friends/family. |
| Sharing with other organisations | -Check there is a legal reason for sharing the data with a third party.  -Check they are GDPR compliant and consider completion of a Data Protection Impact Assessment. | -Assume other organisations will keep data safe. (If you have provided the data you also have a responsibility to make sure it is not lost). |
| Emailing data | -Use encryption and make sure the email address is correct before sending.  -Use BCC when sending emails to external parties so that email addresses are hidden.  -Only use the school email address. | -Use group emails when sharing sensitive data.  -Don’t make any comments that you would not expect the person to be able to read if they asked for copies of the email. |
| Disposal | -Ensure that once the data is no longer required it is disposed of appropriately. | -Use standard waste disposal routes for the disposal of personal data. |
| Data Breach | -Report any suspected breach to the school Business Manager immediately it is discovered. | -Hope that the breach will not be found or is unimportant. (Every breach must be identified and managed). |
| Individual Rights Request (Subject Access Request) | -Confirm the identity of the person making the request and their right to the information.  -Monitor any request through the use of the school’s form. | -Release the information without checking that any redactions have been completed where required. |
| Data Protection Officer | -Ask the school DPO for help and advice if a requirement is unclear. (Phone or email at any time to gain support). |  |

**OFFICE STAFF** – please take particular care of the following risks.

|  |  |  |
| --- | --- | --- |
| **Activity** | **Do** | **Don’t** |
| Computer passwords | -Keep passwords secure | -Share access details with other staff. |
| Breach management | -Ensure you know what a breach looks like and where they can occur. | -Ignore a breach – they must be recorded and managed. |
| Individual Rights Request | -Ensure the right person has been made aware of any request for personal information.  -Help the data subject to refine their search to what they really need. | -Delay dealing with a request, a response is required within a month.  -Try to gather all the information requested without first agreeing the scope of the request. |
| Personal data storage | -Keep personal data secure on password protected computers or in lockable files. | -Leave computers with open programmes unattended.  -Leave hard copy files on unattended desks. |
| Record retention | -Ensure you know how long different records must be retained.  -Ensure you have a system in place for annual removal of surplus data. | -Keep files past their retention period unless there is a real risk that they will be required in the future. |

**TEACHING STAFF** – please take particular care of the following risks.

|  |  |  |
| --- | --- | --- |
| **Activity** | **Do** | **Don’t** |
| Emails about pupils and parents | -Use initials instead of full names where possible / appropriate. | -Include personal comments that may be embarrassing for the person to read. |
| Computer access | -Ensure passwords are kept secure and cannot be guessed. | -Let a pupil use your computer. |
| Photographs of pupils | -Ensure you know who has not given consent for pupil images to be used by the school. | -Use a child’s image unless consent has already been given or requested. |
| New teaching apps | -Ask the DPO to confirm if a new app is compliant with GDPR before you use it. | -Provide pupil information without having a legal reason to provide it. |
| At home | -Ensure data is kept safe between school and home.  -Keep laptops out of sight in an unattended car.  - Keep information safe at home.  -Access data through a secure portal when possible. | -Download personal information onto a personal device.  -Print and store personal information at home.  -Use any form of encrypted or unprotected device. |