Rosebank School

Listening, Responding, Learning

DATA HANDLING/DATA SHARING POLICY/PROCEDURE

DATE OF THIS POLICY:	**NOVEMBER 2019**
Ratified by Governors:	**05/12/2019**
Frequency of Update:	**Annually**
Due for Revision:	**November 2020**
Person Responsible:	**Carina Baylis**

Data Handling

The management of personal data is done in accordance with the statutory requirements of the Data Protection Act 2018.

1. Personal data

As part of their role, staff will have access to some personal data concerning children and their families including, but not limited to; names, dates of birth, the name of their parents or guardians, address and contact numbers as well as legal information and curricular data. Sensitive information may also be held in accordance with our safeguarding policy.

2. Responsibility

School

- It is the school's responsibility to ensure that the data handling policy is followed by the members of the establishment and that they also respect the Data Protection Act 2018

Staff

- The staff are responsible for their safe handling of the children's, the staff's and any potentially sensitive, data. Staff need to adhere to the Data Protection Act of 2018.

Governors

- As with members of the school staff, governors need to adhere to the same rules as other members of staff when, as part of their role, they have access to data.

3. Registration

School will renew their data protection registration as a Data Controller on the Data Protection Register, held by the Information Commissioner's Office, every year as per the Data Protection Act 2018.
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

4. Data storage and disposal

Securely Accessing and Storing Data

ICT systems and MIS are managed in such a way that protected files can be given permission levels, with protected files being hidden from unauthorised users. Access to data is granted as required for the employee's role only.

Personal and sensitive data is only to be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). Autolock should be enabled when devices are left unattended.

The school encourage users to have strong passwords, which are changed regularly. User passwords must never be shared.

Storage media is stored in a secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment must not be used for the storage of personal data. Where personal devices are used to access data remotely passwords should not be stored on the device and personal data should not be downloaded.

When personal data is stored on any mobile device or removable media:

- the data must be encrypted and password protected,
- it must have virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (see guidance below) once it has been transferred or its use is complete.

The school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material is held in lockable storage, either on or off site.

The school recognises that data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests.

Secure transfer of data and access out of school:
On occasion it may be necessary for personal data to be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Before removing or copying sensitive, restricted or protected data the user must gain permission from the data controller and ensure the media is encrypted and password protected and is transported and stored securely.
- If data is to be taken or transferred to another country, particularly outside Europe, advice should be taken from the Data Protection Officer in this event. For example, staff should not take such data on holiday unless there is a justifiable need and permission has been sought.

Data Disposal:
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

5. Training and CPD

Training normally takes the form of an induction, as well as annual training as part of Safeguarding. Any relevant updates involving the emergence of new technology will be given as they arise.

6. Data Breach and reporting incidents

Logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy.

All significant data protection incidents will be reported through the DPO to the Information Commissioner's Office.

Guidance

Managing data in compliance with the Act

There are three broad stages of processing data that you need to be aware of to ensure personal data is handled appropriately:

- gathering data
- keeping data
- disclosing data.

Data Security

Keeping data secure is essential to complying with the Data Protection Act. Security is also essential when working away from school and on personal or mobile devices.

Specific guidance

Gathering data - You must comply with the Data Protection Act whenever you gather or collect personal data for school-related purposes. There are three general rules of compliance that you should follow when collecting data.

- Identify an appropriate legal basis
- Limit the Personal Data you collect
- Keep data secure

Limit the personal data you collect - the school must ensure it only collects personal data that is strictly necessary, especially sensitive personal data. Any irrelevant or excessive information should not be retained.

Keep data secure - All personal data gathered must be held securely. We will restrict access to data and maintain confidentiality by:

- only allowing staff to access the data if necessary
- taking care not to lose data
- ensuring data is kept securely, whether on or off the school site.

Keeping data - If you have access to existing files or data you must follow the rules on keeping data to ensure that requirements of the Data Protection Act are met. There are four general rules of compliance that you should follow when keeping data.

- review the content of files and records
    - accuracy
    - relevance
    - fairness and access rights
- keep data secure
- maintain best practice in record keeping
    - limit access to data
    - only use data for the original purpose
    - keep files in a single location

- only retain data for as long as necessary

Review the content of files and records

Accuracy - Files and other records containing personal data must be kept up-to-date and regularly checked for accuracy. Record any changes and delete any obsolete information.

Relevance - Only relevant and necessary information should be retained. Carry out the regular administration of files and records to remove duplicated materials and irrelevant information.

Fairness and access rights - Individuals have the right to see their personal data, including any comments about them. Opinions about individuals in documents should be justifiable and based on fact. It is permissible to give a reasoned, frank opinion about a student's work or behaviour, but not to express personal dislike or make any insulting or defamatory remarks. Do not record, however informally, comments you would not be happy for the Data Subject to see.

Keep data secure - All paper and digital records containing personal data must be held securely. You must take care to ensure that data cannot be accessed or viewed by anyone not authorised to do so.

Maintain best practice in record keeping

Limit access to data - Access to personal data should be restricted to those staff who require access for legitimate business or operational reasons and used for the purpose(s) for which it was granted. Exercise caution if you are asked by a third party to disclose personal data.

Only use data for the original purpose - Personal data collected for one purpose may not subsequently be used for another without the knowledge of the data subject.

Keep files in a single location - All documents which may need to be referred to in order to carry out normal business should be kept centrally in a single file. Members of staff holding their own separate files can only be justified if it is in the interests of the student or other individual, for example where the information is particularly sensitive.

Private files should not be routinely kept so as to avoid duplication or fragmentation. Personal data should only be reproduced for specific purposes. Once the purpose is fulfilled the record should be securely disposed of.

Subject Access provisions apply to 'private' files in the same way as to any other records. Any additional or separate files maintained by staff or governors relating to students for the duration of a programme of study should be weeded after this has finished.

Storing selected work-related or staff records at home or in a personal email account does not exempt them from the Subject's right of access.

Only retain data for as long as necessary - Personal data should not be kept for any longer than is necessary. Refer to the school's Retention Policy for more information. When personal data is to be deleted or disposed of, ensure that confidentiality is maintained. Paper files should be put into the confidential waste bin or sacks provided.

Disclosing data - Individuals are entitled to see all information held about themselves, but personal data should only be disclosed to third parties under specific conditions. If you are concerned about a request for data, contact the Data Protection Officer for advice.

Be open with individuals - Wherever possible, be open with individuals in relation to information held about them. If an individual wants to make a formal Subject Access Request under the Data Protection Act, they should be referred to the Data Protection

Take care with requests from third parties - Exercise caution if you are asked to disclose information about an individual to someone else, either within or outside the school. You can pass on information to other members of staff if they legitimately require the information for their duties, but in most other cases you must not disclose personal data without an appropriately identified legal basis. In some cases, even parents may not be entitled to information without the Data Subject's consent. See the school's subject access request policy for further details.

The school may receive requests for information from bodies such as the police and the Inland Revenue. If you routinely disclose such data as part of your job, you should first take steps to ensure that requests are genuine and legitimate. All non-routine requests should be referred to the Data Protection Officer via the Data Protection Lead.

Disclosing information in an emergency - Personal information can be disclosed in an emergency. In such a situation, if necessary, personal information can be disclosed without consent. For example, if a member of staff or a student collapses and is unconscious, it would be permissible to inform medical staff that the individual suffers from diabetes.

Disclosing data to third parties - You must exercise caution when dealing with requests for personal information from outside the school and any queries should be referred to the Data Protection Lead/Officer.

Disclosure formats

Personal data should only be disclosed over the telephone in emergencies. When personal data is included in an email, the email should be password protected and where appropriate encrypted.

Requests from public and official bodies - When dealing with routine type queries from public and official bodies, such as Local Education Authorities (LEAs) or equivalent, you need to be convinced that:

- the person is who he/she says he/she is
- the enquiry is genuine
- the student in question is clearly identified.

If in doubt as to the authenticity of the enquiry, seek advice from the Data Protection Lead.

Unless you are familiar with named staff at the organisation in question, it may be advisable to ask for a main switchboard number to phone them back to ensure the legitimacy of a query.

Requests in writing should be on official headed paper. Keep a record of all telephone calls with any other correspondence and a copy of the outgoing letter.

Requests from the police - The police do occasionally ask for personal data as part of an inquiry but they don't have the automatic right to receive information about our staff or students. You should not be pressured into handing over personal information. There is a special process to allow the police to access personal information.

Requests from other third parties – Requests from third parties, should be referred to the Data Protection Lead to assess.

Third party processor - If the school has to disclose personal data to a third party, either for them to process data on our behalf (for example, to conduct a questionnaire for us) or as part of an agreement we have entered into with them (for example, sending student data to another institution about exchange students), the school must have a written contract in place with the other party.

The contract will ensure that the third party processor will only process the personal data in accordance with our instructions and will comply with the Data Protection Act. The Data Protection Officer can draft data sharing agreements when needed. Contact the Data Protection Lead for further information.

Sending personal data outside the European Economic Area (EEA) - The Act states that personal data should not be sent to countries outside the EEA which do not have an adequate level of data protection unless the individual consents or there is other good reason as set out under the Act, for example, for the performance of a contract between the individual and the school. Contact the Data Protection Lead for further information.

Data security

Any information you access when conducting school business that pertains to living individuals is covered by the Data Protection Act. More stringent rules apply to sensitive personal data containing information such as a person's race or ethnic origin, religious beliefs or health.

Keeping data secure

The most common causes of data loss or leakage and breaches of the Act can be avoided by following our guidance.

Keep personal data secure

- paper files should be kept in locked cabinets or locked offices when not being used and stored securely at the end of the day - not left on desks.
- offices should be locked when left unattended
- always ensure that you log off from your computer when away from it.
- password protection should be used for any electronic files/documents containing sensitive personal data.
- take particular care when transferring personal data onto a memory stick, laptop or any other mobile device - use password protection and encryption where appropriate.
- if you ever need to include sensitive personal data in an email use password protection or encryption where appropriate.
- change your password frequently and adhere to any school ICT Policy.
- don't copy any personal data unless it is strictly necessary.

Restrict access to personal data

- ensure the access to data is only granted to staff who require it for legitimate purposes.
- don't disclose personal data to other third parties.
- avoid third parties seeing digital screens displaying personal data.
- if you need to share data with a third party for business purposes contact the Data Protection Lead so that a data sharing agreement can be entered into with them.

Storing personal data

- where possible, store/save personal data on the school server.
- never store personal data, especially sensitive personal data, on a mobile or home computer unless it is strictly necessary and the device has been encrypted where appropriate.
- don't store or transfer personal data where it could be lost or exposed (on unencrypted USB drives, mobile devices and laptops).

Dispose of personal data carefully

- Dispose of paper files securely using the confidential waste bin or sacks
- If you store personal data on your own device you must securely erase all personal data on it before disposing of it.

Report data breaches - You must immediately report breaches or potential breaches as soon as you become aware of them. This includes lost or stolen laptops, memory sticks or other mobile devices, and accidental disclosures of information, for example sending an email to the wrong recipient.

Email security - Only use your school email account for school related business.

Taking data offsite - Reduce risks of a breach of the Act through data loss by:

- limiting the amount of personal data taken off-site - only take the data you really need
- making and using a copy of your data rather than taking the original
- anonymising data wherever possible to remove Sensitive Personal Data.

Use encryption and passwords - If you store or transfer personal data onto a mobile device or pc outside of the schools IT systems, ensure that password protection and encryption where appropriate are used.

Take security measures - If you store personal data on a PC or device outside the schools's IT systems, it should be as a short-term measure only. Keep a copy of the data on the school's IT system too, so that if a device is lost or stolen, you do not lose the only copy.

Store it on the school's IT system at the same time or transfer it there as soon as possible. In any event, the data should be deleted from the device/PC outside the school's IT system as soon as possible.

Take special care when transporting personal data to and from your home and when using public transport.

Responding to a request for information

Any staff member who receives a request for information, which they believe to be a request for data under the Data Protection Act, should immediately forward the request to the Data Protection lead.

You should pass on all such requests where any person is essentially asking for information about themselves, even if they do not mention the Data Protection Act. The exception is where the request is for information that would normally be released as a matter of course..

Photography and filming

Images of individuals, whether in still photographs or moving film images, will often be caught by the definition of personal data in the Data Protection Act. In many cases, consent from the individuals will need to be obtained in order to process (capture and use) the images fairly and lawfully.

If you are unsure as to whether the Act applies to the photos or film that you plan to take, get advice from the Data Protection lead.

Photo Consent

Taking and using photographs or film footage of people without their consent could constitute a breach of the Act. If an individual objects to the display of their photograph, then it must be removed.

Withdrawing consent

An individual captured in an image can withdraw their consent even after having signed the consent form. Any such withdrawal should be in writing.

Once consent is withdrawn, the school cannot use the relevant images again, but it will not normally be possible to recall documents in which the image has already appeared.

Data Sharing

Where we share information regularly with organisations such as the Council, Department for Education etc there will be a defined process in place and in most cases such sharing will be covered by a data sharing agreement – a document that states the expectations in relation to what will be shared, when and how.

If we provide information to a data processor to allow them to undertake work on our behalf, this will be covered by contract or a Data Processing Agreement.

If we have one off or irregular requests to share information there is no formal process in place and so we will have to determine whether we can share, what to share and why.

Checklist - Systematic Data Sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have we assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue we are addressing?
- Could the objective be achieved without sharing personal data?

Do we have the power to share?

Key points to consider:

- The type of organisation we are.
- Any relevant functions or powers of our organisation.
- The nature of the information we have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If we decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, our data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What we need to tell people about the data sharing and how we will communicate that information.
- Measures to ensure adequate security is in place to protect the data.

- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Checklist - One off requests to share Data

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do we think we should share the information?
- Have we assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do we have concerns that an individual is at risk of serious harm?
- Do we need to consider an exemption in the DPA to share?

Do we have the power to share?

Key points to consider:

- The type of organisation we are.
- Any relevant functions or powers of our organisation.
- The nature of the information we have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If we decide to share

Key points to consider:

- What information do we need to share?
    - Only share what is necessary.
    - Distinguish fact from opinion.

- How should the information be shared?
    - Information must be shared securely.
    - Ensure we are giving information to the right person.

- Consider whether it is appropriate/safe to inform the individual that we have shared their information.

Record your decision

Record our data sharing decision and our reasoning – whether or not we shared the information.

If we share information we should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Our justification for sharing.
- Whether the information was shared with or without consent