Doddinghurst Infant School

Church Lane, Doddinghurst, Brentwood, Essex, CM15 0NJ

Data Protection Policy

Date last reviewed:	Spring 2019
Frequency of review:	Annually
Date next review due:	Spring 2020
Version:	1.2

General rules in complying with Data Protection law

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals.
2. ***MUST***: Where personal data is used we must make sure that the data subjects have access to a complete and current **Privacy Notice.**
3. ***MUST:*** We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which processes personal data.
4. ***MUST***: We must process only the **minimum** amount of personal data necessary to deliver services.
5. ***MUST***: All employees who record **opinions** or intentions about service users must do so carefully and professionally.
6. ***MUST***: We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. ***MUST***: We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition.
8. ***MUST***: Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. ***MUST***: Consent will **expire** at the end of each 'Key Stage' period unless it is reconfirmed.
10. ***MUST***: We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
11. ***MUST***: If we receive a **request** from a member of the public or colleagues asking to access their personal data, we must handle it as a Subject Access Request.
12. ***MUST***: If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we must fully consider Data Protection law before disclosing it.
13. ***MUST***: When someone contacts us requesting we change the way we are processing their personal data, we must consider their **rights** under Data Protection law.
14. ***MUST NOT***: You must not access personal data which you have **no right to view.**

15. ***MUST***: You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so.
16. ***MUST***: You must **share** personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer.
17. ***MUST***: Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice.
18. ***MUST***: All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
19. ***MUST***: When using **'data matching'** techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate.
20. ***MUST***: We must maintain an up to date entry in the **Public Register of Data Controllers.**
21. ***MUST:*** Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we must follow the relevant procedure.
22. ***MUST NOT***: You must not **share** any personal data held by us with an individual or organisation based in any country outside of the European Economic Area.
23. ***MUST***: We must identify **Special Categories** of personal data and make sure it is handled with appropriate security and only accessible to authorised persons.
24. ***MUST***: When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method.

Why must I do it?

1. To comply with legislation
2. To comply with Data Protection legislation this requires us to make the data subject aware of how we will handle their personal data.
3. To ensure that the rights of the Data Subject are protected in any proposed new activity or change to an existing one.
4. The law states that we must only process the minimum amount of information needed to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
5. To maintain professional standards and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
6. To comply with a principle of Data Protection law.
7. To comply with Data Protection law. Where processing does not rely on a legal condition other than consent.
8. When using personal data for marketing and promoting services it is unlikely that any lawful condition other than consent would apply.
9. Consent can only be valid for a reasonable period of time.
10. To comply with the right to access personal data.
11. To comply with the rights of the Data Subject under Data Protection law.

12. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so.
13. To comply with the legal requirements to keep personal data secure but also to ensure that where there are legal grounds to share information in a managed way that this is done correctly.
14. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed e.g. to investigate alleged criminal activity or breaches of Organisation policy etc.
15. To comply with a principle in Data Protection law and the Data Protection Officer Governance requirements.
16. To comply with the Data Subject's rights.
17. This is a regulatory requirement and allows the public to see what personal information we hold to support transparency.
18. Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law.
19. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here. The member states of the EEA share common legislation which provides assurance to us that personal data will be securely handled under the same provisions that exist under the Data Protection Act.
20. To comply with Article 9 of GDPR
21. To comply with Article 9 of GDPR and comply with a principle of Data Protection law requiring personal data is processed with appropriate security measures

How must I do it?

1. By following the points in this policy.
2. By approving and reviewing a compliant privacy notice in line with the Privacy Notice Procedure and making it available to the data subjects.
3. By completing and approving a Privacy Impact Assessment or Data Protection Impact Assessment where the processing is 'high risk' to the rights of the data subjects.
4. By ensuring that the means we use to gather personal data (such as forms etc.) only ask for the information that is required in order to deliver the service.
5. By considering that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy.
   For example, there should be at least an annual check of the currency of data held about service users and whenever contact is re-established with a service user, you should check that the information you hold about them is still correct.
6. By following the points in the Consent Procedure. Parents/ Guardians of pupils in the last year of a key stage should expect a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date then consent should be assumed to be no longer valid.
7. By following the points in the Records Management Policy. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas.

8. By following the points in the Statutory Requests for Information Policy. We must be aware that data subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.
9. By following the points in the Statutory Requests for Information Policy. Such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law if for a criminal investigation; however, the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law.
10. By reviewing the impact of any requested change on any statutory duty being fulfilled by the Organisation.
11. By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to personal data. You must inform your manager if you have access to data which you suspect you are not entitled to view.
12. By ensuring appropriate security controls are in place and rules to support those controls are followed. The following should be in place:
    - technical methods, such as encryption, password protection of systems, restricting access to network folders;
    - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
    - organisational measures, such as:
        - Providing appropriate induction and training so that staff know what is expected of them
        - Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
        - Making sure that passwords are kept secure and forced to be changed after an agreed period and are never shared.
13. Consult your manager, any procedure guidance or any library of sharing agreements managed by the Organisation. Consult the Data Protection Officer in one-off cases of sharing.
14. By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and in what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016).
15. By completing compulsory training courses relevant to your role. Records will be kept of induction training and annual refresher training. Training content for each role will be determined by feedback on current training methods and the outcome of investigating security incidents. This will be reviewed frequently.
16. By ensuring an Impact Assessment has been approved for the activity.
17. The entry should be reviewed annually and an update is to be made when any change to the purposes of processing personal data occur.
18. Follow the guidance in the Data Minimisation Procedure.
19. Consult the Data Protection Officer over any proposed sharing outside of the EEA. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data in a nation outside the EEA, this must be first approved by a Privacy Impact Assessment.

20. Special Categories of Personal Data are information revealing *racial or ethnic origin*, *political opinions*, *religious or philosophical beliefs*, or *trade union membership*, and *genetic data*, *biometric data* for the purpose of uniquely identifying an individual, *data concerning health* or *data concerning an individual's sex life or sexual orientation*. Where this data is held it should be stored securely and in a way that access is restricted only to those internal staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data and through secure means.
21. Hard-copy packages must be marked as such by writing on the exterior of the package. Emails should contain the wording in the 'subject' field before the email title. Refer to the Records of Processing Activity document and the register of Data Flows for clear instruction on how you are expected to handle sending the data securely according to the particular activity you are undertaking.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting SIRO (Senior Information Risk Owner) - Headteacher

Document Control

Version:	1
Date approved:	January 2018
Approved by:	Finance and Resources committee
Next review:	January 2019

References

- Data Protection Act 2018 (including the General Data Protection Regulation 2016
- Article 8, The Human Rights Act 1998
- Investigatory Powers Act 2016

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.