

Chantry Community Primary School

Data Protection and Information Security Policy

Date adopted by the governing body	8 th October 2018
Date to be reviewed	October 2020

6. Policy statement:

Chantry Primary School is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with the principles that personal data will be:

- processed lawfully, fairly and in a transparent manner
 - collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way (*'purpose limitation'*)
 - adequate, relevant and limited to what is necessary for the purpose for processing (*'data minimisation'*)
 - accurate and where required, rectified without delay (*'accuracy'*)
 - not be kept in an identifiable form for longer than necessary (*'storage limitation'*) i.e. in line with the school's retention schedule
 - information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures (*'integrity and confidentiality'*). This includes:
 - using appropriate means of transmitting data
 - secure storage / disposal of personal information
 - where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract
- See the school's Information Security Policy for more information on securing personal data.

Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 12)
- not be transferred to countries outside the European Economic Area without adequate protection

7. General Statement

Chantry Primary School is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so

- health,
- sex life/orientation
- genetic/biometric identifier

Information that is **confidential** but doesn't relate to an individual or individuals includes the following:

- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the school or another organisation. This could be personal, financial, reputation or legal damage.

11. Data Protection by Design

Whenever a new policy, procedure, system or database involving personal data is proposed a Data Protection Impact Assessment (DPIA) will be completed. This will be used to identify and reduce any risks to privacy and potential risks of harm to individuals through the misuse of their personal information.

The school also recognise that in some circumstances it will be mandatory to conduct a DPIA where processing is likely to result in a high risk to individuals.

12. Data Subject Rights

Any person wishing to exercise their rights under data protection legislation can do so by emailing or writing to the school - details of which can also be found on the school's Website.

Requests will be processed within 1 month of receipt of the request unless the request is complex (or if multiple requests are received from the same person)

Examples of when a request may be considered complex:

- it involves retrieval and appraisal of information from multiple sources
- it involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been refused or cannot be obtained

In these cases a 3 month deadline for responding to the request will apply. For complex requests likely to take over 1 month, the applicant will be notified of this within the initial 1 month period.

Right to restriction

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the school processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the school in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

Right to portability

Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object

Data subjects have the right to object to their information being processed in the following circumstances:

- If the school has decided that processing is necessary either to
 - a) perform a task carried out in the public interest or
 - b) as part of the school's official authority or legitimate interest and the data subject feels this is not applicable.Information about why the school is processing information (the legal justification) can be found in the school's privacy notice.
- If the school retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the school will cease processing for this purpose if an objection is raised.

If the school uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- availability (ensuring that authorised users have access to relevant information when required)
- relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff
- we will report and follow-up all breaches of information security, actual or suspected

Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information.

System operating procedures will be developed and maintained to ensure compliance with this policy.

Information systems are checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

15. Management of Information

The School will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the school:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

15. School records

We will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the school's Records Management and Electronic Records Management policies.

16. Contacts

Data Protection Officer

Peter Questier	East Sussex County Council	Cs.dpa@eastsussex.gov.uk
----------------	----------------------------	--

Office of the Information Commissioner

The Information Commissioners


Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Website: www.ico.gov.uk


8/10/18