2018

TOFT HILL PRIMARY SCHOOL
Data Protection Policy and Toolkit May 2018

Schools handle increasing amounts of personal information and have a statutory requirement to comply with ***the EU General Data Protection Regulation ("GDPR")*** *and any domestic data protection legislation (currently the Data Protection Act 1998, but with a new Data Protection Bill currently going through Parliament). Together these will be referred to as "the Data Protection Legislation" in this note.*

Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner's Office ("ICO"). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach, which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

This policy has been amended from a Durham County Council sample policy to meet the requirements and reflect the arrangements of this individual school. All guidance from the ICO is adhered to and incorporated into policies and procedures of the school. It is accepted that DCC accepts no responsibility for a school failing to comply with the Data Protection Legislation based on an interpretation of this sample policy.

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- how staff, parents and pupils can access personal data.

1.1. It is a statutory requirement for all schools to have a Data Protection Policy:

(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

1.2. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In Addition article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

2. Lawful Basis for processing data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

2.1 Age. Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13 this responsibility is transferred to the child and parents will not have responsibility for their child's data. (This is subject to the Data Protection Bill becoming law. The 'default' age under the GDPR is 16.)

2.2 Consent. If there is a lawful basis for collecting data then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

RIGHTS

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For “privacy notices” covering the right to be informed, please see section 5 below.

Different rights attach to different lawful bases of processing:

	Right to erasure	Right to portability	Right to object
Vital Interests	✓	**X**	**X**
Legal Obligation	X	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓
Contract	✓	✓	**X**
Consent	✓	✓	X but right to withdraw consent

The right to erasure. GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with information about which data can continue to be legally held if a data subject asks to be ‘forgotten’. Schools’ data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that where a school relies on either a ‘legal obligation’ or a ‘public task’ basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school’s data retention guidelines.

3. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a “Potential Data Breach” which could result in legal action against the school. The loss of sensitive, or “special category”, personal data is considered much more seriously and the sanctions may well be more punitive.

3.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

3.2. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff (SEND)
- (Some information regarding safeguarding will also fall into this category) staffing e.g. Staff Trade Union details

Note – See section on sharing information.

3.3. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the

forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provides additional information on their website. See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

4. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection, they should appoint a Data Protection Officer to manage data.

4.1. Risk Management – Roles: *Data Protection Officer*

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

In some schools other staff may have been delegated responsibility for particular issues, for instance the handling of SEND information.

4.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5. Legal Requirements

5.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: http://ico.org.uk/for_organisations/data_protection/registration

5.2. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. This privacy notice will be passed to parents / carers through a letter. More information about the suggested wording of privacy notices can be found on the DfE website:
http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

New privacy notices should be issued to all 'data subjects' by May 2018 even if the data subject has previously received a similar notice. This is because of the new rights in the GDPR that people should be informed about.

6. Transporting, Storing and Disposing of personal Data

6.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

6.1.1. Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only 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) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately 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 (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school / academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (The school will need to

set its own policy, relevant to its physical layout, type of ICT systems etc. Schools need to be aware of a significantly higher risk of a data loss, and should ensure that they can recover from a cyber-attack.)

6.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- the school does not allow storage of personal data on removable devices
- only encrypted removable storage purchased by the school is allowed to be used on school computers.

6.1.3. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

6.1.4. Images

- Images of pupils will not be processed off site and permission for this will be obtained in a photographic permission notice.
- Images will be protected and stored in a secure area.

6.1.5. Cloud Based Storage

- The school / academy has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. See advice from the DfE below:-
- https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

6.2. Third Party data transfers

As a Data Controller, the school / academy 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 as well as data processing agreements. http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

6.3. Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

6.4. Systems to protect data

6.4.1. Paper Based Systems

- All paper based personal data will be protected by appropriate controls, for example:
  - Paper based safeguarding chronologies will be in a locked cupboard when not in use
  - Class Lists used for the purpose of marking may be stored in a teacher's bag.
- Paper based personal information sent to parents e.g. end of term reports (will be checked by the secretary and the headteacher, or deputy headteacher, before the envelope is sealed).

6.4.2. School Websites

- Uploads to the school website will be checked prior to publication, for instance:
  - to check that appropriate photographic consent has been obtained
  - to check that the correct documents have been uploaded.

6.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- Where technically possible all e-mail containing sensitive information will be encrypted by e.g. attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password) or
- The use of Egress (Secure e-mail system) allows for secure communication.

6. Data Sharing

The school is required by law to share information with the LA and DfE. Further details are available at:

https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Durham LSCB also provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

Schools should ensure that, where special category data is shared, it is transmitted securely for instance by secure e-mail such as Egress or is transferred in tamper proof envelopes securely delivered to the recipient.

7. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the data protection officer will inform the head teacher and chair of governors.
- The school will follow the procedures set out in Appendix 5.

8. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes. *GDPR is due to be implemented in May 2018.*

Date: Review: May 2020

Signed:
Chair of Governors

Adopted by the Governing Body on _____

The Data Protection Officer is ___Mrs Leanne Nesbitt

Appendix 1 - Links to resources and guidance

ICO Guidance on GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education
Specific information for schools is available here. This includes links to guides from the DfE

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv
Specific Information about CCTV

Information and Records Management Society – Schools records management toolkit
http://irms.org.uk/page/SchoolsToolkit
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information
Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 - Privacy Notices

These are now a separate attachment

Appendix 3 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR
All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:
The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:
General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:
General information note from the Information Commissioner on publication of examination results.

Education Act 1996:
Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:
Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:
Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:
Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 - Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

- Data protection Officer in place
- Information asset log complete
- School able to demonstrate compliance with GDPR
- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents/pupils aged 13 or over
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests
- If school has CCTV, appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*