Policy: Data Protection Policy

Date: May 2018
Review date: May 2020
Authorised by: Governing Body
Updated by: School Business Manager

Introduction
In order to operate efficiently Upton St Leonards C of E Primary School [the School] has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

Our commitment
As the data controller Upton St Leonards C of E Primary School is committed to ensuring personal information is properly managed and that it ensures compliance with the General Data Protection Act 1998 [GDPR May 2018). The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so in line with the data protection principles and the Data Protection Act (DPA). https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

Scope
The member(s) of staff responsible for data protection legislation will be the Head Teacher with delegated responsibility to the School Business Manager. However the requirements of this policy are mandatory for all staff employed by the school, governors, volunteers and work experience students and any third party contracted to provide services within the school. All staff and contractors must treat all student information in a confidential manner and follow the guidelines within this document, adequate training will be provided to all staff.

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The DPA does not apply to access to information about deceased individuals.

Responsibilities
The Head Teacher with delegated responsibility to the School Business Manager is responsible for ensuring compliance with the DPA and this policy within the day to day activities of the School. The Head Teacher with delegated responsibility to the School Business Manager is responsible for ensuring that appropriate training is provided for all staff.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA.

Personal and Sensitive Data

The DPA stipulates that anyone processing personal data must comply with eight principles of good practice; these principles are legally enforceable and applied to all data processed:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- Shall be accurate and where necessary, kept up to date;
- Shall not be kept for longer than is necessary for that purpose or those purposes;
- Shall be processed in accordance with the rights of data subjects under the Act;
- Shall be kept secure i.e. protected by an appropriate degree of security;
- Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:
https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Notification

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School is registered.

Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breeches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO, in accordance with the GDPR regulations.

Fair Processing /Privacy Notices

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parent and pupils prior to the processing of individuals data.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as 'Children' under legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

On occasion, circumstances may arise where the school is required either by law or in the best interests of pupils or staff to pass information onto external authorities, for example the Local Authority, Ofsted, or the Department of Health. These authorities are compliant with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals with an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition;
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent.

The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed or if the data is in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy-impact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests)
All individuals whose data is held by the school, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

School Business Manager
Upton St Leonards C of E Primary School
Bondend Road
Upton St Leonards
Gloucester
GL4 8ED

No charge will be applied to process the request.

Data Access
Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.
Data may be disclosed to the following third parties without consent:

- Other schools

If a pupil transfers from Upton St Leonards C of E Primary School to another school, their academic records and other data that relates to their health and welfare, will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress as a result.

- Examination Authorities

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- Health Authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- Police and Courts

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- Social Workers and Support Agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- Educational Division

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.
Upton St Leonards will ensure that it only shares data with GDPR compliant service providers supplying Management Information Systems (MIS) and/or Learning platforms in use within the School.

Photographs and Video
With prior consent, images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.
Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources including marketing and social media.
Please note that images will only be taken by staff and/or pupils, normally on portable devices provided by the School, e.g. school owned cameras and iPads.

Subject to the School Leadership Team's priorities and decisions regarding storage capacity, photographs of parents/pupils/staff will normally be held indefinitely for historical archive and marketing purposes. Refer below for information regarding right to be forgotten.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during school activities, on or off-site, without prior consent. In practice, prior to key school events, such as Sports Day, parents are advised to be mindful of taking pictures of children other than their own.

The management of photographs that are published on Social Media sites will be governed by the Terms of Service of the provider. Once published on a Social Media site retrospective deletion of the photograph may not be possible if it has been shared by a third party.

Location of Information and Data

Hard copy data, records, and personal information are stored securely and out of sight. Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have off-site meetings or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should only be taken off the school site under exceptional circumstances. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be confidentially destroyed using the Secure Shredding sacks. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, or other device such as a laptop or tablet, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- Some staff may be issued with a laptop or similar device and are able to remove this from the school site in order to work, for example, at home. When working off-site using such a device, staff must ensure that the window and documents are properly shut down before leaving the device unattended. Sensitive information should not be viewed in a public place or within sight of a third party who is not an employee of the school.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB and saved onto the USB only.
- USB sticks that staff use, must be password protected.
- When 'Cloud' storage is used, access must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal
Upton St Leonards C of E Primary School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.
Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf
The school will use a qualified source for the secure disposal of IT assets and collections.

Retention of Records
Upton St Leonards C of E Primary School is required by law to keep certain records in addition to complying with the Data Protection Act 1998 (incorporating GDPR 2018) and the Freedom of Information Act 2000. The following information has been provided from information provided by the Gloucestershire Archives (GCC). Unless a specific period is shown all record types should be kept until they are of no further administrative use to the school.

Type of Record	**Trigger**	**Minimum Retention period at School**	**Final Action**
Accident Records(children)	Date of Birth	25 Years	Destroy
Accident/injury at work records (staff)	Date of incident	12 years	Review
Accounting records (other than annual accounts)	End of the financial year	6 years	Destroy
Accounts (Annual)	End of financial year	6 years	Archive – deposit at Gloucestershire Archives
Administrative files (routine)	End of administrative use	5 years	Review to see whether a further retention period is required
Admission registers	Date of last entry	6 years	Archive – deposit at Gloucestershire Archives
Attendance registers	End of academic year	3 years	Destroy
Contracts under seal	End of contract	12 years	Destroy
Contracts under hand	End of contract	6 years	Destroy
Contract monitoring records	End of current year	2 years	Destroy
Data Images		Indefinitely.	
Development plans (school)	End of administrative use	6 years	Archive – deposit at Gloucestershire Archives
Free School Meal Registers	End of current year	6 years	Destroy
Governors' reports	Date of meeting	6 years	Archive – deposit at Gloucestershire Archives
Instruments of Government		Retain permanently until closure of school	Archives – deposit at Gloucestershire Archives
Maintenance logs	Date of last entry	10 years	Destroy

Minutes of governors, staff and PTA meetings	End of academic year	6 years	Archives – deposit at Gloucestershire Archives
OFSTED reports and papers	Superseded by new report	Review on replacement by new inspection report	Archives – deposit at Gloucestershire Archives
Policies	Superseded by new policy	Retain in schools whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Archives – deposit at Gloucestershire Archives
Property title deeds and architects plans	No longer used regularly	Permanent	Archives – deposit at Gloucestershire Archives
Pupil files and record cards (primary)	Pupil leaves school	Immediate	Transfer records to secondary (or other primary) school
SAT's/PAN/Value added records	End of academic year	6 years	Destroy
School Prospectus	End of academic year	3 years	Archives – deposit at Gloucestershire Archives
Scrap books and photograph albums	End of administrative use	Immediate	Archives – deposit at Gloucestershire Archives
Special Educational Needs (SEN) Files	Date of last entry in file	30 years then review	Destroy unless legal action pending. Some LA choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education "case.
Special Educational Needs and Disability Act 2001 Section 1: statements	Date of Birth	30 years	Destroy unless legal action pending
Staff – personnel files	End of employment	12 years	Destroy

Right to be forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and that all their personal data is erased by the school including any data held by contracted processors.

It should be noted that for photographs/videos published on a Social Media site retrospective deletion of the photograph/video may not be possible if it has been shared by a third party.

Our appointed Data Protection Officer is Richard Morley, Director, SchoolPro TLC LTD