



Data Protection Policy

Approved and Adopted by Governors on

21.09.2021

Signed

Introduction

We are committed to preserving the privacy of our children, parents/guardians and staff and to complying with the Data Protection Act 1998. To achieve this commitment the personal information that we hold is collected and used fairly, stored safely and not unlawfully disclosed to any other person.

We comply with our duties under the Data Protection Act 1998. We have a School ICT and E-Safety Policy that are kept up to date by the Schools ICT Co-ordinator and Headteacher.

The first priority of this policy at all times is the avoidance of harm or distress to individuals.

In order to operate efficiently, we have to collect and use information about children, parents/guardians and staff. This personal information is handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

All staff who process personal information must ensure that they follow the Eight Data Protection principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- Handling all personal data (for example – pupil attainment data, images) with reference to this policy.
- Ensuring that they do not access data unless they are required to / have good reason to be accessing it in line with the duties of their post.

The Principles of the Data Protection Act

The Act stipulates that anyone processing personal data must comply with eight principles of good practice. These principles are legally enforceable.

The principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. 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.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. 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.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- that data;
- that data and other information (including any images from which the individual can be identified) which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information about:

- racial or ethnic origin;
- religious or other beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- criminal proceedings or convictions.

Rights to Access Personal Data

The Data Protection Act allows individuals to place a Subject Access Request (SAR) to see the information held about themselves in electronic and in paper records.

There is also a separate right for parents to access their child’s education record - the Education (Pupil Information) (Wales) Regulations 2004.

Parents are able to access all the information about their child if the child is unable to act on their own behalf or gives their permission. As a general guide, a child of 12 or older is expected to be mature enough to make this kind of request. Therefore Stepside CP School would only allow information to be accessed by a parent or guardian.

All requests for access to personal data must be made in writing to the Headteacher. A request for an educational record must receive a response within 15 school days. The school will apply a charge the cost of supplying a copy of the information but it is free for a parent to view the educational record.

Images

Images are included in the scope of the Data Protection Act where they can be used to identify a living individual. Increasingly, technology is making it easier for pictures and images (including photographs - both digital and film, as well as videos) to be used inappropriately as printed material or on the web and so we have included a specific section in this policy about images. It is important that pictures and images of pupils taken, not only by the school, but also by parents/guardians, external agencies including press and other pupils, are done so in a way that reflects the protective ethos of the school.

We recognise that staff will be required to take pictures of pupils for curriculum purposes ranging from Foundation Phase through to Year 6. The guidance outlined within this policy applies to curriculum (including assessment), extra curricular activities, publicity and celebrating achievement.

Using children's images can be motivating for the pupils involved, provide crucial evidence for assessment and provide a good opportunity to promote the work of the school. At Stepside CP School, we will aim to make full and proper use of images whilst complying with the law and preserving the safety of children.

We also recognise that parents and other family members will wish to take images of our pupils during open events e.g. Christmas concerts, class assemblies, sports days. Again, the school aims to preserve the safety of children.

The taking of visual images during school activities is not prohibited by the Data Protection Act if these are taken for **personal** use and not uploaded onto the internet, including Social Media eg Facebook.

However, written and informed consent **must** be obtained from all parents/guardians of pupils whose images they intend to **publish** anywhere. These may include:-

- Printed publications including external and internal publications e.g. school magazines, annual report, newsletters;
- School notice boards; ie display boards in public areas of the school;
- Media – including newspapers and TV.

On our school website:

- photos will not be captioned with the children's full names;
- personal details of children such as e-mail address, home address and telephone number will not be revealed on the website;
- no individual child will be identifiable to a visitor to the school.ie. a visitor would not be able to come in and ask for a child by name and class using information from our website.
- general shots of classroom or group activities are preferable to close-up pictures of individual children.

Permission from Parents/Guardians

Parents/Guardians will be required to complete a personal information form on admission to our School which will include a permission slip for the use of images in school, in press releases and on the school website. The Headteacher has a list of all pupils whose parents have not given full permission and this list will be made available to those working with the children concerned.

Images taken by Visitors at School Events

The Information Commissioner states: "The Data Protection Act is unlikely to apply in many cases where photographs are taken in school. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure."

However, the school does have a duty to ensure, as far as reasonably possible, that such photos and videos are used for personal use only, "for the family album." In particular, that they are not uploaded onto the web. At Stepside CP School, we will remind parents of this before events. Clearly, the school can only go so far in terms of setting out these conditions and does not have control over photographs taken by parents.

The school recognises that some parents may have very good reasons to be concerned that their child may be filmed and are encouraged to speak to the Headteacher who will take advice on whether inclusion in a photograph/video might pose a risk to a child. The school will deal with such situations sensitively and discuss how best to resolve the situation. The aim would be to try and avoid the child being excluded from such activities but the welfare of that child and the rest of children need to be taken into account.

External Photographers

We contract Bluestone Studios to take individual, family, class, team and whole school photos. They are a reputable company and they ensure that the images taken will only be made available to the parents of pupils and the school and they employ safe and secure storage arrangements.

The school may also use the services of a professional photographer to provide images, for example, for the school prospectus. The school will ensure that the photographer has a DBS check and that images are stored safely and securely.

Similarly, a photographer may be used to take images at an event organised by the Friends of Stepside School, for example at the School Prom or Santa's grotto at the Christmas Fayre. Identical guidelines will be followed.

Use of Cameras by Members of Staff

When taking photos of pupils, staff will endeavour to ensure that pupils are appropriately dressed. General shots of classroom/group activities are preferable to close up pictures of individual pupils but it is recognized that, particularly for assessment there may be a need to take more individual images.

Staff will only use school cameras and video recorders. The storage of images is of paramount importance. Storage devices such as school encrypted memory sticks, external hard drives and CDs will be stored safely and securely.

Images taken in school will only be printed in school and then stored appropriately (for example on internal noticeboards, achievements books and in class books.) Discarded prints will be disposed of safely and the school has a shredding machines accessible to all staff.

Staff will refer to the permissions list before publishing photos of pupils on display boards, in newspapers or the school website. The guidelines mentioned previously will be adhered to. Images used for assessment purposes will also be stored safely and securely.

Incidents of inappropriate or intrusive photography should be reported immediately to the Headteacher.

Images taken by Pupils

Pupils are not permitted to use personal mobile devices e.g. phones or tablets in school; they are stored by a member of staff when brought onto school premises. Pupils are also discouraged from bringing cameras to school.

Pupils are permitted to take photos on some school visits and residential trips. The parents and pupils will be reminded that images taken should only be used for personal use and should not be uploaded onto the worldwide web.

Photographs in the Press

Occasionally, a press photographer will take images of the pupils for publicity or information purposes. The school will ensure that pupils whose parents have not given the relevant permission will not appear in such images. In addition, the school will not release full names of pupils to the press i.e. first name and surname.

The School regularly submits images taken in school to the press for publicity and congratulatory purposes and the same guidelines will be followed.

Information Handling

Staff/governors handling personal information about staff or pupils must ensure that:

- personal information is secure and only accessible by those authorised to see it;
- they are mindful of the need not to disclose personal information about others when in discussions with parents;
- personal information is not discussed in public places;
- computers are locked when not attended;
- all portable media e.g. laptops (including removable media) containing personal information is encrypted;
- usernames and passwords for school systems are not shared with anyone else.
- Pupil data and any data transfers are only shared via agreed Pembrokeshire County Council and Welsh Government systems (for example Dewi, G2/Integris. Schools to Schools S2S systems).

Encryption

The Information Commissioners Office recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Data at Stepside School is managed and protected in accordance with the Schools ICT and E-Safety Policy and using best practice and risk assessment guidelines.

Data breach

A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service."

As soon as an information breach is identified the school are required to inform the Senior Information Risk Owner (SIRO) within Pembrokeshire County Council immediately.

Depending on the information supplied a decision will then be made on the next course of action.

Training

All staff employed within the School will be reminded annually about this policy at the beginning of the School term. All Staff (including Teachers, Support Staff, Caretakers and Cleaners) are required to complete the Pembrokeshire County Council e-learning modules on Data Protection and Records Management.

Mr Paul Harries Headteacher, is the nominated Data Protection Officer for the School and Mrs Tina Amphlett is the Governor who takes the lead on Data Protection Issues.

This Policy will follow the information and guidelines issued by Pembrokeshire County Council.

Other Related Policies

- Stepside School ICT , CCTV and E-Safety Policy
- PCC Information Governance Policy
- PCC Subject Access Request Policy
- PCC Subject Access Guidance Notes
- PCC Data Protection – Corporate Guidance Notes (All)
- PCC Data Protection – Corporate Guidance Notes (Supervisors and Managers)
- PCC Protected Emails and Receiving Protected Emails

Further guidance on the Data Protection Act can be obtained from the Information Commissioner's Office (www.ico.gov.uk) and from Pembrokeshire County Council departmental data controller staff.

School and Governors Approval and Review

This policy will be subject to annual review.

First presented to Curriculum Governing Body Committee on Thursday 11th June 2015.

Annual review next review due October 2018

_____ **Rosemary Tippet Maudsley Chair of Governors**

_____ **Paul Harries Headteacher**

(Staff member responsible for Data Protection)

_____ **Tina Amphlett on behalf of Governing Body**

(Governor responsible for Data Protection)