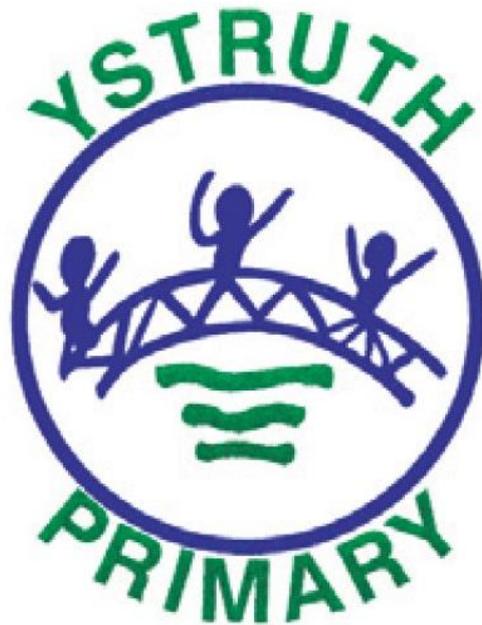


GDPR Policy 2024-2025



Ystruth Primary School
Ysgol Gynradd Ystruth

Adopted by Governing Body: November 2024
Date to be reviewed: November 2025

Ystruth Primary School

Data Protection Policy

Through SLA with BGCBC: Data Protection Officer is Steve Berry

Information Asset Owner is Headteacher; Mel Miller

1 The school will comply with:

General Data Protection Regulation 2016

Data Protection Act May 2018

This policy is used in conjunction with the school's ***E-Safety Policy*** and the **BCCBC GDPR Policy**.

2 Risk of Non- Compliance:

The School's main risks with regard to data fall into two key areas:

Information about individuals falling into the wrong hands, through poor security or inappropriate disclosure of information:

- Accidental loss of data
- Deliberate theft of data
- Lack of vigilance by staff or lack of training

Individuals being harmed through data being inaccurate or insufficient:

- Vulnerable people put at risk
- Inappropriate action taken by the Council, such as incorrect legal action

The School seeks to minimise these risks through the use of appropriate physical and electronic data security, policies, procedures, training and guidance.

3 Data Gathering

3.1 All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.

3.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

4 Data Storage

4.1 Personal data will be stored in a secure and safe manner.

4.2 Electronic data will be protected by standard password and firewall systems operated by the school.

4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.

4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

4.5 Particular attention will be paid to the need for security of sensitive personal data.

5 Data Checking

5.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

5.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

6 Data Disclosures

6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organizations that have a legal right to receive the data without consent being given.

6.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

6.4 Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas and birthdays, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem).

6.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

6.6 Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

6.7 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data.

6.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

7 Subject Access Requests

7.1 If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

7.2 Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

8 Children's Images

8.1 Children's images may be used on the school website, in local media, in performance recordings and in promotional material (e.g. school prospectus). These images will always feature groups of two or more children and will never include names linked to the images.

8.2 Children's images will only be used for above purposes when parents have signed a consent form for the school to do so. This consent will be updated yearly and parents have the right to remove their consent at any time.

8.3 A register of children for whom consent has been refused is held centrally by the school, is updated yearly and should be referenced by staff whenever images are to be used in any of the above manners.

M. Miller

Reviewed November 2024

Chair of Governors:

Review Date Autumn Term 2025