St Paul's Church in Wales Primary School

A family of learners who believe, belong and succeed together.

Teulu o ddysgwyr sy'n credu, yn perthyn ac yn llwyddo gyda'i gilydd.

GDPR Policy

Data Cyffredinol (GDPR)

Staff Responsible: Chris Gascoigne

Agreed: February 2022

Review Date: February 2024

St Paul's Church In Wales Primary School

A family of learners who believe, belong, and succeed together

Our Vision

At St Paul's C/W Primary school we will promote an inclusive, diverse and supportive environment where teachers, parents and members of the community positively impact on children's learning.

At St Paul's C/W Primary School we will provide a safe opportunity for all staff and children to experience learning that impacts on their local community and global communities around the world.

We will nurture a creative learning community at St Paul's Church in Wales Primary school that allows staff and children to reach and expand their potential.

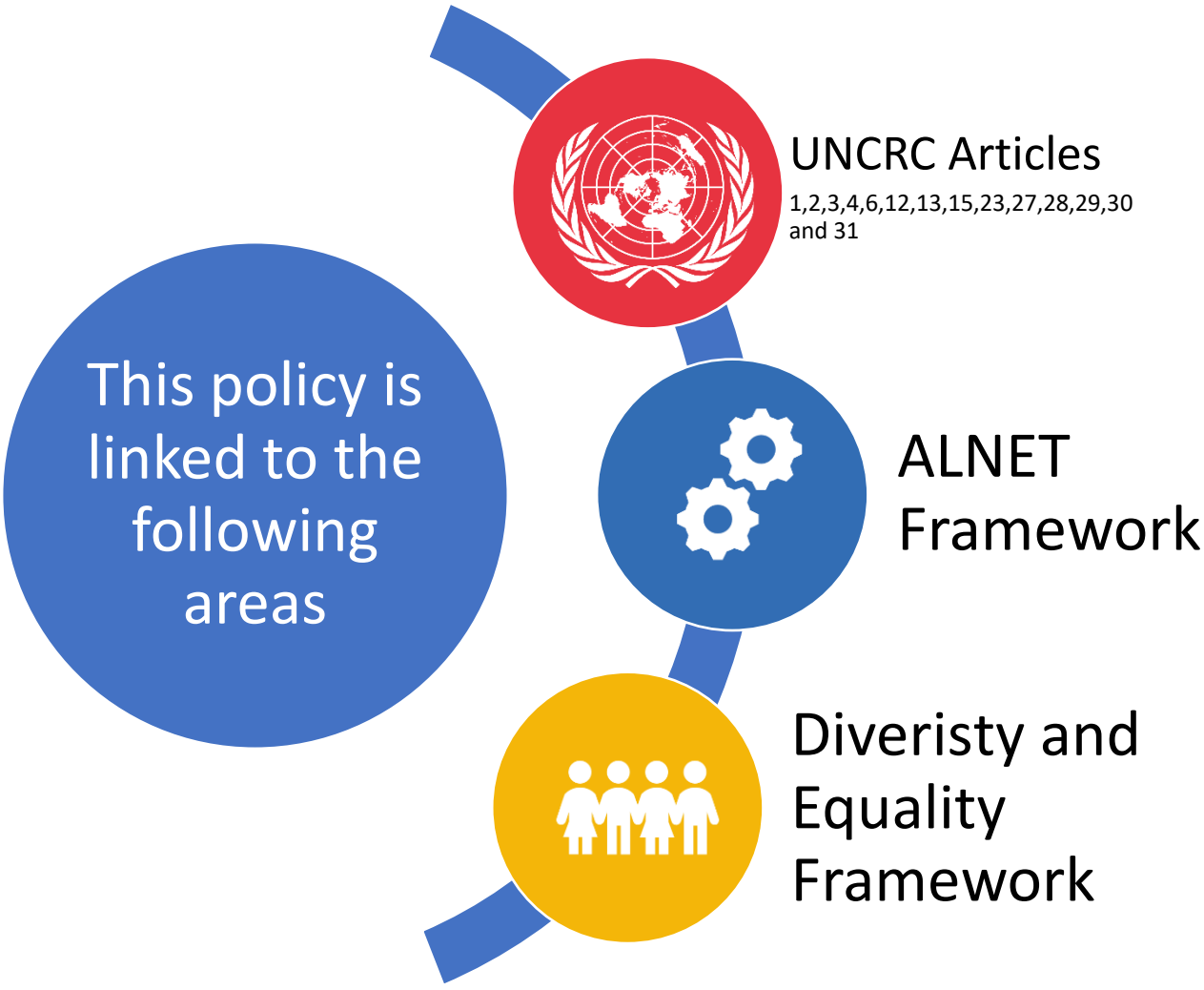
How Will We Achieve This?

To achieve this all staff and governors will:

- Nurture respect and promote good behaviour for others;
- Involve the wide community in the learning environment; and
- Promote excellent communications and relationships between school and home.

St Paul's Church In Wales Primary School

A family of learners who believe, belong, and succeed together



St Paul's Church In Wales Primary School

A family of learners who believe, belong, and succeed together

Data Protection Policy

Introduction

St Paul's Church in Wales Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide Education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

Schools have a duty to inform individuals including parents and pupils of the information that it holds. This should summarise which information the school holds, why it is held and any other parties to whom this information may be passed on to. Schools will advise individuals through Fair Processing in concise, transparent, plain language and will be free of charge.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation (GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held as defined within the GDPR.

General Data Protection Regulation (GDPR) Principles:

The GDPR establishes six enforceable principles that must be adhered to at all times in that information must be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible for those purposes.

3. Adequate relevant and limited to what is necessary in relation to the purpose for which it is processed.
4. Accurate and where necessary kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than necessary for purposes that which the personal data is processed.
6. Processed in a manner that ensures appropriate security of the personal data.

General Statement

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

- Inform individuals why the information is being collected when it is 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.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as:
    - Right of Access
    - Right of Rectification
    - Right to Erasure
    - Right to Restrict Processing
    - Right to Data Portability
    - Right to Object
- Ensure our staff are aware of and understand our policies and procedures.
- Ensure our staff are provided with adequate training and support.

Rights of access to information

There are two distinct rights of access to information held by Schools about pupils:

1. Under the GDPR any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2011.

Individual Rights

The GDPR provides the following rights for individuals:

1. **The Right to be Informed**

The school will provide concise, transparent, intelligible and easily accessible information about the processing of personal data to individuals via the Privacy Notice. This will be written in clear plain language and will clearly set out how personal data is processed within the school.

2. **The Right of Access**

The school will provide individuals with access to their personal data and supplementary information; this will be processed as a Subject Access Request. Subject Access Requests will be free of charge and processed in line with the statutory requirements and timeframes.

3. **The Right to Rectification**

The school is committed to rectifying personal data if inaccurate or incomplete and notifying any relevant third parties of this.

The school will respond to a Request for Rectification within one month of receiving the request, if the Request for Rectification is deemed complex, this will be responded to within two months.

If the school cannot take action in response to a Request for Rectification, it will provide a written explanation of this. An individual will then have a right to complain to the schools Data Protection Officer.

4. **The Right to Erasure**

The school will consider individual requests for deletion or removal of personal data where there is no compelling reason for its continued processing.

Schools will inform relevant third parties of erasure of personal data; unless it is impossible, or involves disproportionate effort to do so.

5. **The Right to Restrict Processing**

The school will ensure that data processing is restricted in any of the following circumstances:

- Where an individual, or individuals contest the accuracy of personal data until the accuracy is verified.
- Where an individual has objected to the processing.
- When processing is unlawful.
- If the school no longer needs to, or is required to keep the personal data but the individual requires the data in relation to a legal claim.

If data processing is restricted, the school will notify any relevant third parties.

6. The Right to Data Portability

The school will comply with individual requests to data portability free of charge and within one month of receiving the request.

7. The Right to Object

The school will comply with an individuals right to object and will stop processing personal data unless there are compelling legitimate grounds for processing or the processing is in relation to a legal claim.

The school will inform individuals of their right to object at the point of first communication in the schools Privacy Notice.

8. Rights in Relation to Automated Decision Making and Profiling

The school will not use automated decision making nor profile any individuals.

The school clearly sets out within its Privacy Notice what information we collect/use and why this is relevant.

Subject Access Requests

The school will process all subject access requests and provide a copy of the information free of charge and within one month of receipt. This is limited by law however to work that takes more than eighteen or more hours to produce or incurs a cost to the school of £450 or more.

The school will charge a fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Further copies of the information can be provided at a reasonable charge.

If requests are complex or numerous the school has the right to extend the period of compliance by a further two months. The school will notify individuals if this occurs.

If a request is manifestly unfounded or excessive the school has the right to refuse the request. The school will notify the individual and explain why they cannot comply with the request and will inform the individual of their right to complain to the schools data protection officer.

The school will verify the identity of the individual making the request using reasonable means.

Complaints

Complaints in relation to processing of personal data should be addressed to the schools data protection officer.

Review

This policy will be reviewed on an annual basis. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mr C Gascoigne on 02920 235854 who will also act as the contact point for any requests for personal data.

Further advice and information is available from the Information Commissioner's Office:

www.ico.org.uk

The Information Commissioners Office
Wycliffe House
Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: **0303 123 1113** – Helpline is open from 9am to 5pm, Monday to Friday

Email: casework@ico.org.uk

Appendix

Raising Awareness

Within a school, there are all sorts of job roles that utilise personal data for a variety of reasons. For example, some staff will be responsible for ensuring they simply use data responsibly, others will be making significant decisions about what data is used, how it is processed and stored and who it is shared with and how. As such, it is likely that a 'one size fits all' approach to staff training will not work.

In their discussions with schools the Information Commissioners Office (ICO) believe the following to be an effective approach and encourage schools to think about **3 levels of raising awareness:**

1. **All staff** should be aware of what personal data actually is; what 'processing' means in the broadest form and what their duties in handling personal information are. All staff should be aware of the processes by which they are permitted to use that information, and be **clear of the scope of the permitted usage of that data**. They should be engaged with the **risks around data getting into the wrong hands,** and their responsibilities regarding responding to a **data breach.** The job roles that might warrant this level of training include catering staff, welfare supervisors, library staff, cleaners, first aiders etc.
2. **Those who can influence how data is uses, processed and secored.** By this we mean any staff in school who may have the authority to create and store data; enter data into applications/software or decide if/when they will process certain data. These individuals may also have responsibilities for how paper documents are handled within the school environment. This likely covers all teaching staff as a minimum.

   As well as the awareness work, staff should have the chance to **review the high-level data maps produced by the school**, and be given an opportunity to contribute the different perspectives that they offer compared with senior leaders or data leads.

   Staff should also be engaged with things like **ensuring there is a legitimate and lawful basis and, if relevant, a condition for processing** the information they utilise, and that **storage of data is minimised** to that required to perform the necessary tasks.

   Staff should be engaged in **discussions about identification and the mitigation of risks**, and know the governance arrangements that oversees the management of risks**.** In addition, as more schools process and store personal data by electronic means, schools will want to produce user- friendly security policies and staff training to help reduce the risk of a data breach. The job roles that warrant this level of training may include, but are not limited to, higher level teaching assistants, teaching staff, office staff, site administrators, information and communications technology (ICT) staff and technical support staff. Everyone can help prevent data loss by following basic cyber security steps.
3. **Senior leaders and e Seniorleadersandexecutivelevel,andthosewhomanagethe'data ecosystem'.** By this, we mean those in school who are responsible and accountable for making choices around the use of technology and its security, deciding on what and how the data is shared, and setting school policies around the use of data and technology. As well as the senior leadership team (SLT), it may well be network managers or business managers. These people need to be **sufficiently aware of the content of GDPR and the Data Protection Act, so that they can assure governors that the school has the right things in place to be compliant.** As a data controller the school has a responsibility to ensure that there is accountability, and transparency throughout the whole data ecosystem and that the principles of data minimisation and privacy by design are adhered to by all parties, and that any contracts with data processors cover the relevant areas of data protection. This level of training is aimed at those who are accountable for those responsibilities on a day-to-day basis.

Job roles warranting this level of training include, but may not be limited to, all SLT members, curriculum leads, business managers, ICT leads and data managers and MAT executive teams.

In addition to staff training, **awareness for governors and MAT trustees** should focus on the following areas:

- That the ultimate responsibility and accountability for compliance sits with governors and trustees. Data Protection will, on an ongoing basis, require resourcing and governors/trustees will be an important support mechanism for the DPO in performing his or her role
- Making sure their school has good network security to keep the personal data they hold protected. This should also include having a business continuity plan in place that has cyber resilience as a consideration.
- That the new legislation moves schools from being required to 'comply' with data protection, to being required to 'demonstrate' compliance with legislation.
- To actively demonstrate compliance, schools need to document all their assets containing personal data and ensure they are being appropriately managed and secure.
- Appraising and scrutinising the performance of the school leadership/executive in the area of data protection
- Preparation requires a thorough 'audit' or 'housekeeping' exercise on current data processes that should already be in place in relation to the Data Protection Act. In particular, it is likely that data retention policies need more consideration.

- Following the data audit, an assessment of risks to data protection that will be considered by the school to be high or medium should be maintained. Schools should clearly identify what these risks are and how they are being addressed. This could include identifying any shortcomings in the school's network security infrastructure and keeping IT security policies up to date. This should be documented as evidence towards compliance.
- Schools need to review how they communicate their use of data with pupils/parents, and the rights of data subjects, with clear explanations regarding the strengthened rights (including Subject Access Requests (SARs)). Schools need to have agreed procedures for dealing with SARs.
- A need to appoint a Data Protection Officer who has the ear of governors (and vice versa) and is somewhat independent from but can work closely with the management structure that develops and maintains data policies. (Step 7 has more information).
- A review of data protection policies in light of any changes to procedures and processes arising from the data audit and risk management.
- Reviewing data protection is an ongoing process requiring the whole school to be continually mindful of their responsibilities. Formally scheduling an annual review of current practice through an internal or external audit may be something schools wish to consider.