CARDIFF
CAERDYDD

Western
Learning
Federation

Riverbank School

PRIVACY STANDARDS POLICY

Riverbank
SCHOOL
Learning together to be the best we can

RATIFIED BY GOVERNORS	14th July 2021
DATE REVIEWED	14th July 2021
DATE FOR REVIEW	14th July 2023
DATE PUBLISHED	July 2021

Monitoring the policy

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

SIGNED **DATE**

Chair of Governors

SIGNED **DATE**

Executive Headteacher

SIGNED **DATE**

Deputy Executive Headteacher

SIGNED **DATE**

Head of School

The values and principles

The federation is underpinned by a set of values that define the culture of the three federated schools.

Our Principles

Honesty

Responsibility

Positivity

Trust

Empathy

Patience

Respect

Kindness

Our Values

- We celebrate our differences.
- We have a shared sense of belonging.
- We play, laugh, smile and celebrate success.
- We have a positive attitude.
- We learn from experiences to develop life and independent skills.
- We follow our dreams and aspirations.
- We care for our own and wider environment.
- We improve quality of life.

Definition

Values	One's judgement of what is important in school life.
Principles	Morally correct behaviour and attitudes.

Rights Respecting Schools

Every child has rights "without discrimination of any kind, irrespective of the child's or his or her parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status"

Western Learning Federation
Executive Headteacher - Mr Wayne Murphy
Deputy Executive Headteacher - Miss Rachel Faulkner
Tel: 029 2083 8560
E-mail: westernlearningfederation@cardiff.gov.uk

Riverbank School
Head of School - Mrs Deborah Herald
Tel: 0292 0563 860
E-mail address: riverbanksp@Cardiff.gov.uk

Tŷ Gwyn School
Head of School - Mr Jamie Brortherton
Tel: 0292 0838 560
E-mail address: tygwynsp@cardiff.gov.uk

Woodlands School
Head of School - Mrs Siân Thomas
Tel: 0292 0838 560
E-mail address: woodlandshighschool@cardiff.gov.uk

Riverbank SCHOOL
Learning together to be the best we can

Tŷ Gwyn SCHOOL
Learning to achieve

Woodlands SCHOOL
Learning for Living

Vincent Road, Cardiff, CF5 5AQ

Western Learning Federation
Together we learn, grow and achieve

@CardiffWestern @RiverbankSch @GwynSchool @WoodlandsHS

www.westernlearningfederation.co.uk

CONTENTS **PAGE**

APPENDICES

1. Introduction

The purpose of this policy is to set out Riverbank's internal Privacy Standard. It has been created in accordance with the requirements of the Data Protection Legislation including the EU General Data Protection Regulations, and the Information Commissioner's Code of Practice's on data protection compliance.

This Privacy Standard outlines how the school will comply with the principles and legal conditions the school must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of our operations and activities, including pupil information, supplier and employee data. This policy aims to outline the standards expected to be abided by School Personnel that provides a service requiring the use of personal information.

The school has appointed a Data Protection Officer in Accordance with Section 4 Article 37 of the GDPR who is responsible for implementing and updating this policy.

2. Interpretation

The following definitions have been used throughout this policy:

Automated Decision-Making:	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.
Automated Processing:	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
School Personnel:	All employees, workers, contractors, agency workers, consultants, directors, members and others.
Consent:	An agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Data Controller:	The person or organisation that determines when, why and how to process Personal Data. The school is the Data Controller of all Personal Data relating to our School Personnel and Personal Data used in our organisation for our own business purposes.
Data Subject:	A living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights

	regarding their Personal Data. They will include employees, parents, pupils, customers, complainants and residents of the borough.
DPIA:	Tools and assessments used to identify and reduce risks of a data processing activity. Data Protection Impact Assessments can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
Data Protection Legislation:	The General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, in the UK and any successor legislation to the GDPR or the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2426/2003*) and all applicable laws and regulations relating to the processing of personal data and privacy, including the guidance and codes of practice issued by the Information Commissioner.
Data Protection Officer:	The person required to be appointed in specific circumstances under the GDPR.
Explicit Consent:	Consent which requires a very clear and specific statement (that is, not just action).
Personal Data:	Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach:	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design:	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Data Protection Legislation.
Privacy Notices:	Separate notices setting out information that may be provided to Data Subjects when the school collects

	information about them.
Processing or Process:	Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised:	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Special Category Data:	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. Objective

This policy sets out what we expect from School Personnel in order for the school to comply with the data protection law. Compliance with this policy is mandatory. Related policies are available to help interpret and act in accordance with this policy. School Personnel must also comply with all such related policies.

This policy has been created in order to minimise the risk of processing Personal Data in a manner which Data Subjects do not approve of. It provides practical advice on how school Personnel should collect, record and store consent in accordance with the Data Protection Legislation. This policy sets out what Data Subjects can expect from the school when processing Personal Information. School Personnel must read, understand and comply with this Privacy Standard when Processing Personal Data on the school's behalf and attend training on its requirements.

This policy should be used and read in conjunction with the relevant policies and procedures listed in Appendix 1.

4. Scope

This policy covers the processing of Personal Data and Special Category Data and it applies to all School Personnel.

5. Policy Statement

The school takes seriously its statutory responsibilities and will, at all times, act in accordance with the Data Protection Legislation and take necessary and proportionate action in these types of matters. In that regard, the Data Protection Officer, is duly authorised by the school to keep this policy up to date and to amend, delete, add or substitute relevant provisions, as necessary.

6. Data Protection Principles

The school will adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

The school including School Personnel are responsible for and must be able to demonstrate compliance with the data protection principles listed above. This will in turn demonstrate that the school is Accountable for our processing activities that include the use of Personal Data and Special Category Data.

I. Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

School Personnel may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Legislation restricts the school's actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the schools parents, pupils, customers, clients and employees. The Data Protection Legislation allows processing for specific purposes, which are set out below:

(a) the Data Subject has given Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests;
(e) to carry out our public tasks;
(f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notice

The school must identify and document the legal ground being relied on for each processing activity and record this in our Register of Processing Activities in accordance with the Council's Fair Processing Policy.

Consent:

School Personnel must only process Personal Data on the basis of one or more of the lawful bases set out in the Data Protection Legislation, which include Consent. Consent must be obtained in accordance with the school's Consent Policy.

Transparency (Notifying Data Subjects):

The Data Protection Legislation requires School Personnel to provide detailed, specific information to the Data Subject (your pupil, parents, clients, customers and employees) depending on whether the information was collected directly from the Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

School Personnel must comply with the school's Fair Processing Policy and draft Privacy Notices in accordance with said policy for each processing activity performed.

II. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

School Personnel cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and have consented where necessary.

III. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

School Personnel may only process Personal Data when performing job duties or where

the schools business needs requires it. School Personnel cannot process Personal Data for any reason unrelated to their job duties.

School Personnel may only collect Personal Data that is required in order to perform their job duties; School Personnel must not collect excessive data. School Personnel must ensure any Personal Data collected is adequate and relevant for the intended purposes.

School Personnel must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the school's data retention guidelines.

IV. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

School Personnel will ensure that the Personal Data use and held is accurate, complete, kept up to date and relevant to the purpose for which we collected it. School Personnel must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. School Personnel must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

V. Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

School Personnel must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which the school originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The school will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

School Personnel will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the school's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

School Personnel will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

7. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

The school will develop, implement and maintain safeguards appropriate to our business needs, available resources, the amount of Personal Data that we own and maintain and identify risks (including use of encryption and Pseudonymisation where applicable). The school will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. School Personnel are responsible for protecting the Personal Data we hold. The school will implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. School Personnel must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure.

School Personnel must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. School Personnel may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

School Personnel must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a business need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

School Personnel must comply with all applicable aspects of Information Security Policies and Procedures. Additionally all school Personnel will comply with and not attempt to circumvent the administrative, physical and technical safeguards the school implements and maintain in accordance with the Data Protection Legislation and relevant standards to protect Personal Data.

8. Reporting A Personal Data Breach

The Data Protection Legislation requires the school to notify any Personal Data Breach to the Information Commissioner's Office and, in certain instances, the Data Subject.

The Data Protection Breach Policy details how school Personnel should deal with any suspected Personal Data Breach.

If any school Personnel know or suspect that a Personal Data Breach has occurred, they should not attempt to investigate the matter but should immediately contact the Information Governance Team and follow the Data Protection Breach Policy. School Personnel should preserve all evidence relating to the potential Personal Data Breach.

9. Transfer Limitation

The Data Protection Legislation restricts data transfers to countries outside the European Economic Area in order to ensure that the level of data protection afforded to Data Subjects by the Data Protection Legislation is not undermined. School Personnel will transfer Personal Data originating in one country across borders when it is transmitted, sent, viewed or accessed in a different country.

School Personnel may only transfer Personal Data outside the European Economic Area if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which the school transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;
(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) the transfer is necessary for one of the other reasons set out in the Data Protection Legislation including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

10. Data Subject's Rights And Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;
(b) receive certain information about the schools Processing activities;
(c) request access to their Personal Data;
(d) prevent the schools use of their Personal Data for direct marketing purposes;
(e) ask the school to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of the school's legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling;
(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights

and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

School Personnel must send copies of the requests listed above to the Council Information Governance Team for consideration. School Personnel must not allow third parties to persuade school Personnel into disclosing Personal Data without proper authorisation from the Information Governance Team.

School Personnel must immediately forward any Data Subject request received to the Data Disclosure and Records Officer and comply with the Data Subject Access Request Policy.

11. Accountability

The school must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The school is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The school must have adequate resources and controls in place to ensure and to document Data Protection compliance including:

(a) appointing a suitably qualified Data Protection Officer, who is based in the Information Governance Team, and an executive accountable for data privacy, the Senior Information Risk Owner, their contact details are listed in appendix 2;

(b) implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessment where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(d) regularly training school Personnel on the Data Protection Legislation. The school will maintain a record of training by school Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12. Register of Processing Activities

The Data Protection Legislation requires the school to keep full and accurate records of all our data Processing activities. These will be held in a Records of Processing Activity Register (ROPA).

The schools ROPA will include, the name and contact details of the school and the Data Protection Officer, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data transfers, the Personal Data's retention period and a description of the security measures in

place.

School Personnel must keep and maintain accurate corporate records reflecting the school's Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the school Consent Policy.

13. Training and Audit

The Information Governance Team will ensure all school Personnel have undergone adequate training to enable them to comply with Data Protection Legislation.

School Personnel must undergo all mandatory data privacy related training and Heads of Services must ensure their departments complete the mandatory training in accordance with the Information Security Policies.

School Personnel must regularly review all the systems and processes under their control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

14. Privacy by Design and Data Protection Impact Assessment (DPIA)

The school is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

School Personnel must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of Processing; and
(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

The school must also conduct DPIAs in respect to high risk Processing.

School Personnel should conduct a DPIA, and discuss the findings with the Data Protection Officer, when implementing major systems or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
(b) Automated Processing including profiling and Automatic Decision Making;
(c) large scale Processing of Special Category Data; and
(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the school's legitimate interests if appropriate;
(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
(c) an assessment of the risk to individuals; and
(d) the risk mitigation measures in place and demonstration of compliance.

School Personnel must complete the schools standard DPIA template when the activity involves the processing Personal Data, and a complex DPIA should be completed when the activity involves processing Special Category Data. The DPIA template is located within the Information Governance Team's intranet pages.

15. Automated Processing and Automated Decision-Making

Generally, Automatic Decision Making, including profiling, is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;
(b) the Processing is authorised by law; or
(c) the Processing is necessary for the performance of or entering into a contract.

If Special Category Data is being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is based solely on Automated Processing (including profiling), then Data Subject's must be informed of their right to object. This right must be explicitly brought to the Data Subjects attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

The department that will perform the Automated Processing must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or Automatic Decision Making activities are undertaken.

16. Direct Marketing

The school is subject to certain rules and privacy laws when marketing to our Data Subject's.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a Data Subject opts out their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

17. Sharing Personal Data

School Personnel are not permitted to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

School Personnel may only share the Personal Data internally if the recipient has a business requirement to know the information and the transfer complies with any applicable data transfer restrictions.

School Personnel may only share Personal Data with third parties, such as our service providers, if all of the following conditions are met:

(a) they have a business requirement to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(d) the transfer complies with any applicable cross border transfer restrictions; and
(e) a fully executed written contract that contains approved third party data processing clauses has been obtained.

All data sharing and outsources data processing activities should be approved by the Data Protection Officer and Information Security Officer prior to the commencement of the processing.

18. Breaches of this Policy

If a breach of this policy has been detected it must be reported to the Information Governance Team for investigation.

Failure to abide by the rules and procedures written in this policy will be classed as a breach of this policy and may also be a breach of the Data Protection Legislation.

Breaches of this policy will be considered in accordance with the school's disciplinary policies and procedures and may result in disciplinary action up to and including dismissal.

19. Legal Considerations

In creating this policy the school has given due regard to the following Legislative frameworks:

The Human Rights Act 1998 – Article 8 of this Act gives a right to respect for private and family life, home and correspondence. This Policy does not intend to infringe any Article 8 rights.

The Data Protection Act 2018 – This Act provides a legal framework which sets out how information relating to employees, parents, pupils, customers, clients etc. can be collected, handled and used. This Policy aims to set out how the school will comply with data protection across all school departments.

The General Data Protection Regulations – the GDPR provides that processing personal information must be done in accordance with the lawful bases for processing personal information. It provides a universal standard on what data subjects should expect from data controllers when their personal information is being processed.

The Regulation of Investigatory Powers Act 2000 – This Act covers the extent to which the school is able to monitor and record private communications received within our telecommunication systems. It applies to all public and private communications networks. The school will abide by these Regulations and will not unlawfully intercept communications.

20. Implementation Responsibilities

The Information Governance Team shall develop, maintain, and publish processes to achieve compliance with this policy.

School Personnel will be aware of and adhere to all other relevant policies and procedures.

The head teacher shall be responsible for implementing this policy within their areas of responsibility.

21. Policy Review and Maintenance

This policy shall be reviewed annually and at times as dictated by operational needs and changes in the Data Protection Legislation.

22. Policy Acceptance

All staff must confirm acceptance and adherence to the Privacy Standards Policy and must confirm that they have read and understood the contents of this policy.

PRINT FULL NAME: _____

JOB TITLE: _____

SIGNATURE: _____

DATE: _____ / _____ /_____

Cardiff Council

Privacy Standard Policy – Appendices

1. Relevant Policies
2. Data Protection Contact Officers

Appendix 1

Agreement to the Privacy Standards Policy, also confirms agreement and adherence to the following supporting operational policies:

Consent Policy
Data Protection Breach Policy
Subject Access Request Policy

Appendix 2

The relevant officers responsible for data protection compliance include:

Katie Weaver
Data Protection Officer
Information Governance Team

Needs to be added
Senior Information Risk Owner
Deputy Chief Executive