West Kirby Grammar School
Data Protection and Privacy policy

Purpose
This document is a statement of the aims and principles applied by West Kirby Grammar School (WKGS) to ensure the correct handling of personal data relating to staff, pupils, parents and governors.

Contents
This document covers the following topics:

1. Policy Statement
WKGS needs to keep certain information about its employees, students and other users to allow delivery of education, management of staff and students, and compliance with legislation. The Governing Body has overall responsibility for the maintenance, security and access control of personal data, and is committed to making sure the School complies fully with the General Data Protection Regulations (GDPR) which came into effect May 2018 and replaced the previous Data Protection Act 1998.

2. Definitions
Consent. Freely given, informed, specific to circumstances. There can be two kinds: explicit and implicit. The latter may suffice in some cases, although the Information Commissioner advises that explicit consent should be sought wherever possible.

Data Controller [West Kirby Grammar School]. A person or corporate body who determines the purposes and manner in which any personal data is to be processed.

Data Manager [Gill Kenyon] and Network Manager [Neil Attwood]. Persons with responsibility for retention and deletion of data within specific areas.

Data Processor Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject. Any living individual who is the subject of personal data.

Designated Data Controllers [Head Teacher; Network Manager, Data Manager and the Assistant Head with responsibility for Safeguarding]: Individuals who discharge the responsibilities of the Data Controller on day to day matters.

Erasure. Redaction or 'blacking out' of data.

Personal data. Information relating to an identifiable living individual that is processed as data. The act applies to all data held electronically or in structured files and would include all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, NI numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Processing. Anything at all done to personal data, including but not limited to collection, use, disclosure, destruction and merely holding personal data.

Recipient. Anyone who receives personal data, except the Data Controller, Data Subject, or Data Processor.

Sensitive Personal Data. Information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

Biometric data. Information that relates to statistical measurement made on the human body for identification purposes such as fingerprints scanning used for our Cashless Catering System.

3. Scope

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.

4. Data Protection Principles

WKGS will comply with The Eight Data Protection principles when processing personal data. These require that personal data is:

- Fairly and lawfully processed
- Processed for specified and limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with the right of data subjects
- Kept secure
- Not transferred to other countries without adequate protection

5. Responsibilities

The School as a body is the Data Controller under the GDPR, and the Governors are therefore ultimately responsible for implementation.

Day to day matters will be dealt with by the Designated Data Controllers. The School has four Designated Data Controllers: These are the Head Teacher, Network Manager, Data Manager and the Assistant Head with responsibility for Safeguarding.

All School staff have a duty to comply with this Policy, firstly with regard to the management and security of data they use, but also for the accuracy of their own personal data as held by the School. All staff must:

- Ensure that any information provided to the School in connection with their employment is accurate and the School is kept informed of any changes.
- Follow the Data Protection Code of Conduct when collecting, storing or processing data.

Staff who regularly handle personal data as part of their job receive Data Protection awareness training specific to their role.

6. Subject Consent and Authorised Disclosure

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the GDPR, direct consent must be obtained. For staff, agreement to the School processing some specified classes of personal data is a condition of acceptance of employment. In line with the safeguarding responsibilities the School holds, this includes information about previous criminal convictions. This is detailed on the School's Job Application forms and on the Contract of Employment.

For children and carers, the School seeks consent through a variety of means. The School's privacy statement below explains how personal information is used, shared and held, who it may be shared with and how further information can be obtained. Specific consent is obtained for storage of Biometric (fingerprint) data and use of personal images. During enrolment, carers authorise the School to hold and process information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual. Where information that is more sensitive is to be held, WKGS will seek specific consent.

In certain circumstances, the School is required to disclose personal data. Examples of this would include:

- Where the disclosure is for the purposes of preventing or detecting crime.
- Where the disclosure is required by law or by a court order.
- Where the disclosure is required to safeguard an individual.

7. Data Management and Security

To support compliance with the GDPR, WKGS applies rules for management and security of personal data.

Collection of personal data

Staff members must give careful consideration to the data protection principles before collecting personal data. If consent is not clearly given via the School's privacy statements then explicit consent must be sought. Where any doubt exists, advice must be sought from a Designated Data Controller before collecting personal data.

Secure storage of personal data

Staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage as detailed below:

- Personal data in paper format must be stored in a locked room or cabinet and sensitive personal data kept behind two locks (e.g. in a locked cabinet in a locked room) when not being used.
- Data in electronic format must be stored on a network drive (not local hard drive) where it is password protected and regularly backed up; or
- If a copy is kept on a School USB drive or other removable storage media, that media must itself be kept in a locked filing cabinet.

Ordinarily, personal data should never be stored at staff members' homes, whether in paper or electronic form, on laptop computers or other personal portable devices. It would be seen as reasonable to store students' school work for marking, which contained the students' name and form, at a staff members' home but staff must take personal responsibility for its security.

Processing Sensitive Information

Those processing sensitive information must be sufficiently trained to understand its sensitivity and how it must be treated. Permission from a Designated Data Controller is required before sensitive information can leave the School premises or be shared with an external agency. It must be encrypted, transported securely and stored securely. Sensitive information in electronic format must be stored in limited access areas of the School file structure and password protected. Paper copies are to be kept behind two locks (e.g. in a locked cabinet in a locked room) when not being used. Those processing sensitive information should avoid using computer monitors or desks that could give others sight of the data.

Publication of Personal Information

Before publication of any personal data, care must be taken to ensure:

- Specific consent is obtained or the publication is adequately covered by previously given consent.
- The publication is required to meet the legitimate needs of the School.

Staff should note that unauthorised disclosure of personal information will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

In the event of a data breach, whereby an individual is likely to suffer some form of damage, such as through identity theft or confidentiality breach, the Data Controller or Designated Data Controller must notify the ICO within 72 hours of the breach.

Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Managers should base decisions on data retention on the retention guidelines that start on page 34 of the current version of the 'Information Management Toolkit for Schools' produced by the IRMS.

8. Rights to Access Information

All staff, carers and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act and the GDPR

The School will, upon request, provide any staff, carers or other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, carers and other users have a right under the GDPR to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request (SAR) Form and submit it to the School who then will run the process of generating a report from the School Information Management System and collating any other paper-based documentation. The School will waive a charge for this task on the first application but will make a £10 charge on subsequence applications by the same party. The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the GDPR.

It is the responsibility of the parent or carer to keep the information held by the School up to date. Initial data is collected from the primary or previous school and with a first data collection. The SIMS app has the facility to edit and update information held on the School Information Management System which is monitored by the data processors.

In order to comply with the GDPR the School has derived several policies which are available on request via email: office@wkgs.net or in writing to the Headteacher, Mrs E Sargent.

9. Enquiries

Enquiries about Data Protection or requests for information should be made as follows:

- Staff enquiries to the Data Manager
- Carer enquiries to the Data Manager via Reception Staff

The Head Teacher should be notified of all Subject Access Requests.
Any member of staff, carer or other individual who considers that this policy has not been followed in respect of personal data about themselves or their child should raise the matter with the Headteacher. In the unlikely event that the School is unable to provide a response that satisfies concerns raised, a complaint can be made directly to the Information Commissioner for an assessment.

10. Further Information

For more information on how the data sharing process works between the school and Department for Education please click here.
For information on which third party organisations pupil data has been provided, please click here
For information regarding how the Department for Education collects and shares information here
For further information regarding organisations you can ask for information from, click here and how to make a freedom of information request (FOI Request), click here
For information regarding Microsofts Office365 Retention Policy click here

Public Communications Unit, Department for Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Department for Education: https://www.gov.uk/browse/education
Information Commissioner's Office: ico.org.uk
Information and Records: http://irms.org.uk/page/SchoolsToolkit

Other policies which work alongside the Data Protection and Privacy Policy include:
IT Misuse Policy
Confidentiality Policy
Freedom of Information Policy
In order to access any other School policies please contact the school office on 0151 632 3449 or by email at office@wkgs.net

Privacy Notice for Students *Appendix A*

General Data Protection Regulations - How We Use Pupil/Student Information

Under the Data Protection Act 1998 and General Data Protection Regulations, West Kirby Grammar School (WKGS), as a Data Controller, is required to inform you of what data we collect, store and share in relation to your daughter/son/ward.

The categories of pupil information that we collect, receive, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Contact details (address, email and telephone numbers)
- Exclusion and achievement/behaviour information
- Medical and special educational needs information
- National curriculum assessment results and qualifications, including Learning Records Service unique learner number (ULN)
- Safeguarding information from agencies
- Destination after leaving the School

Data is provided by various sources including; parents/carers, previous schools, Learning Records Service, Safeguarding/Child Protection Agencies, Local Authority and/or the Department for Education (DfE). We use this personal data to:

- Support our pupils' learning
- Monitor and report on their progress
- Provide appropriate pastoral care
- Assess the quality of our services
- Comply with the laws regarding data sharing

WKGS collects and uses pupil information under Article 5 of the Data Protection Act/GDPR to ensure data is:

- Fairly and lawfully processed
- Processed for specified and limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with the right of data subjects
- Kept secure
- Not transferred to other countries without adequate protection

Whilst the majority of pupil information you provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information or if you have a choice.

We hold pupil data in line with the WKGS retention policy, we do not retain records longer than is necessary.

We routinely share pupil information with:

- Schools that the pupil attends after leaving us
- Our local authority
- The Department for Education (DfE)
- Youth support services
- Careers advisers
- NHS

CCTV Cameras

WKGS maintains a small network of security cameras for the detection and prevention of vandalism or in the event of a break in. These cameras record images which are stored securely on the School premises. Only authorised personnel have access to this system and images are not stored for any longer than is reasonably necessary. Cameras are clearly identified with signage as you enter the camera zone. Please refer to the Schools' CCTV Policy for more details.

Youth Support Services

Once our pupils reach the age of 13, we pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. This enables them to provide youth support services, post 16 education and training provider information and careers advice.

A parent/guardian can request that **only** their child's name, address and date of birth is passed to the provider of Youth Support Services in this area by informing the school office in writing. This right is transferred to the child once he/she reaches the age 16. For more information about services for young people, please go to our local authority website www.wirral.gov.uk

National Pupil Database (NPD)

The National Pupil Database (NPD) is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to the information we hold about them. To make a request for your personal information, or be given access to your child's educational records, contact Ms G Kenyon, Data Protection Officer, West Kirby Grammar School, Graham Road, West Kirby CH48 5DP or email office at office@wkgs.net .

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- take action regards damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

If you would like to discuss anything in this privacy notice, please contact: Ms G Kenyon, Data Protection Officer, West Kirby Grammar School, Graham Road, West Kirby CH48 5DP or email office at office@wkgs.net.

Privacy Notice for Staff *Appendix B*

General Data Protection Regulations - How We Use Staff Information

Under the Data Protection Act 1998 and General Data Protection Regulations (GDPR), West Kirby Grammar School (WKGS), as a Data Controller, is required to inform you as an employee of what data we collect, store and share.

The categories of staff information that we collect, receive, hold and share include:

- Personal information (such as; name, date of birth, unique teacher, payroll and NI number, professional qualifications and car registration details.)
- Characteristics (such as ethnicity, religion are voluntary but may be stored if disclosed)
- Contact details (address, email and telephone numbers, emergency contact details)
- Employment information (such as pay scale, hours of work, absence record, appraisal and performance records, references, bank details, Disclosure and Barring Service (DBS) outcomes.)

Data is provided by various sources such as; individual staff member, DBS and previous employer and are required to provide employment and comply with employment law and support career development.

WKGS collects and uses staff information under Article 5 of the Data Protection Act/GDPR to ensure data is:

- Fairly and lawfully processed
- Processed for specified and limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with the right of data subjects
- Kept secure
- Not transferred to other countries without adequate protection

We hold pupil data in line with the WKGS retention policy, we do not retain records longer than is necessary.

WKGS are required to share staff information with:

- The Local Authority, Human Resources Service in order to process salaries
- The Department for Education (DfE) for the School Workforce Census

On occasion WKGS may seek legal guidance on employment law. For these purposes personal staff details are not shared.

It is recognised that in order for staff to carry out their duties, they or the School may need to share their work contact details with outside agencies such as; universities, suppliers, safeguarding agencies and curriculum support companies. These details may include; name, position, work email, work telephone number.

CCTV Cameras

WKGS maintains a small network of security cameras for the detection and prevention of vandalism or in the event of a break in. These cameras record images which are stored securely on the School premises. Only authorised personnel have access to this system and images are not stored for any longer than is reasonably necessary. Cameras are clearly identified with signage as you enter the camera zone. Please refer to the Schools' CCTV Policy for more details.

Requesting access to your personal data

Under data protection legislation, staff have the right to request access to the information we hold about them. To make a request for your personal information, or be given access to your staff records, contact Ms G Kenyon, Data Protection Officer, West Kirby Grammar School, Graham Road, West Kirby CH48 5DP or email office at office@wkgs.net .

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- take action regards damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

If you would like to discuss anything in this privacy notice, please contact: Ms G Kenyon, Data Protection Officer, West Kirby Grammar School, Graham Road, West Kirby CH48 5DP or email office at office@wkgs.net.

Administration Use Only:	
Statutory / Non Statutory:	Statutory
Website:	No
GB Committee:	H & S
Document Formulated:	February 2018
Review:	Every 2 years
Date Reviewed by Committee:	15 October 2018
Reviewed Document Adopted by FGB	
Next Review Date:	October 2020