WREKIN

WREKIN COLLEGE
DATA PROTECTION POLICY (CONFIDENTIALITY OF INFORMATION)

WREKIN

DATA PROTECTION POLICY (CONFIDENTIALITY OF INFORMATION)

Contents

The person responsible for this policy, in consultation with key personnel, is the Deputy Headmaster (Pastoral)

This policy and guidelines needs to be read alongside other school documentation including:

- Anti-Bullying and Child-on-Child Abuse Policy
- Behaviour, Rewards and Sanctions Policy
- Code of Conduct for All Staff and Governors
- Complaints Policy
- Conducting Interviews, Searches and Confiscation Policy and Procedures (Pupils)
- E-Safety and Online Safety Policies
- Games and Sporting Activities Policy and Guidelines
- Health and Wellbeing Centre and First Aid Policy
- Risk Assessment Policy
- Safeguarding and Child Protection Policy
- Welfare and Health Policies - Pupils (includes Alcohol and Smoking Policies)
- Wellbeing and Mental Health Policies and Guidelines - Pupils (includes depression, self-harm, eating
- Whistleblowing Policy and Procedure

Other relevant documentation:

- Boarding Mission Statement (available on the school's website, printed in the Parents' Handbook and House Handbooks)
- Boarding Schools National Minimum Standards – September 2022
- Keeping Children Safe In Education – September 2024
- Working Together to Safeguard Children – July 2023

- Parents' Handbook
- The School's Aims and Code of Conduct
- Pupil Handbook (available via the Pupil Homepage (eLearning Hub)

Date document updated	Document updated by	Comments	Location of saved file	Date of next review
July 2016	GNR/SEC	Policy reviewed and amended.	Google Drive	July 2017
July 2017	SEC	No changes made.	Google Drive	2018
July 2018	GNR	Policy reviewed by key personnel and amended in accordance with the Data protection Act 2018	Google Drive	July 2019
July 2019	SEC	Routine changes only.	Google Drive	July 2020
August 2020	SEC	Routine changes only.	Google Drive	July 2021
January 2023	GNR/AWr/SM	Ref. to new NMS & KCSIE (Sept 2022) and in liaison with new IT Manager (SM). New Asst Head (Planning), PMS, to be trained before next policy review (after handover from GNR).	Google Drive	Sept 2023
June 2025	SM	Changes and updates around dates and also switch to a specific CCTV policy to address changes internally for that	Draft in SM Google Drive	June 2025
December 2025	SMN	Update re: disclosure of data and responsibilities for data in respect of Safeguarding	Google Drive	December 2026

DATA PROTECTION POLICY

General Data Protection Regulation

Our Commitment

The Wrekin Old Hall Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA) 2018: https://ico.org.uk/for-organisations/guide-to-data-protection/
Changes to data protection legislation (GDPR May 2018/October 2024) shall be monitored and implemented in order to remain compliant with all requirements, once the most recent changes are brought into law.

The legal bases for processing data are as follows:

a. **Consent:** the member of staff/pupil/parent has given clear consent for the school to process their personal data for a specific purpose.
b. **Contract:** the processing is necessary for the member of staff's employment contract or pupil placement contract.
c. **Legal obligation:** the processing is necessary for the school to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly Dr. Guy Roberts DPO: groberts@wrekincollege.com), Mandy Badesha (CFO, mbadesha@wrekincollege.com) and Steven Morton (IT Manager, mailto: smorton@wrekincollege.com). However, ALL staff must treat all pupil information in a confidential manner and follow the guidelines as set out in this document.

Training and Awareness

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

All staff will receive data handling awareness/training and will be made aware of their responsibilities, as described in this policy, through:

- Induction training for new staff
- Ongoing training and development of IT skills to understanding the risks of phishing/ransomware/ malware and data loss issues via staff meetings, briefings, INSET, and via day-to-day support and guidance from the IT Support team

Notification

Our data processing activities are registered with the Information Commissioner's Office (ICO), as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register. Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr
/key-definitions/

Types of Personal Data Processed by the School

The school may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details;
- Car details (about those who use our car parking facilities)
- Bank details and other financial information, e.g. about parents who pay fees to the school and staff on the school payroll;
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- Where appropriate, information about individuals' health, and contact details for their next of kin;
- References given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils;

- Images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's policy on taking, storing and using images of children);

Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

The school may, from time to time, need to process 'sensitive personal data' regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

The principles of the Data Protection Act 2018 shall be applied to all data processed

Data will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals; and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Fair Processing/Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individuals' data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our pupils or

staff to pass information onto external authorities, for example local authorities, Ofsted, or the Department of

Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information. Any proposed change to the processing of individuals' data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- That would cause serious harm to the child or anyone else's physical or mental health or condition
- Indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- Recorded by the pupil in an examination
- That would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

Addendum to Information Sharing Agreement: Secondary Use of Data

In addition to the original purpose of information sharing outlined in the Child Sexual Exploitation Information Sharing Pathway and Information Sharing Agreement, the parties acknowledge that identifiable information shared by schools and education settings with Telford & Wrekin Council may also be used for the purpose of identifying, assessing, and supporting children and young people at risk of modern slavery, including but not limited to child sexual exploitation (CSE), criminal exploitation, and trafficking.

Telford & Wrekin Council will act as the data controller for this secondary use and will ensure that all processing is compliant with the UK GDPR and Data Protection Act 2018. This includes ensuring transparency, lawfulness, and fairness in the handling of personal data, and maintaining appropriate safeguards for data security and confidentiality.

This addendum should be read in conjunction with the existing Information Sharing Agreement and does not alter the original intent of collaborative safeguarding between schools and the local authority.

Legal and Statutory Responsibilities

- Children Act 2004 (Section 11) places a duty on schools and local authorities to ensure their functions are discharged having regard to the need to safeguard and promote the welfare of children.

  Working Together to Safeguard Children requires all agencies, including education settings, to share information that is necessary, proportionate, relevant, accurate, timely, and secure to protect children from harm.
- UK GDPR and Data Protection Act 2018 provide the legal framework for processing personal and special category data. The lawful basis for sharing under this agreement is:
  - Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
  - Article 9(2)(g) – processing is necessary for reasons of substantial public interest, specifically safeguarding children and individuals at risk.

Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we

shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regula tion-gdpr/security/
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code- of-practice/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and, where required, these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests)

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

The Head
Wrekin College
Sutherland Road
Wellington
TF1 3BH
Email: headmaster@wrekincollege.com

No charge will be applied to process the request.

Note:

1. Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. Pupils aged 16 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case-by-case basis.
2. A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on their behalf. In these circumstances, the school may check with the child that the request is legitimately on their behalf.

Certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts, nor any reference given by the school for the purposes of the education, training or employment of any individual.

Use of Personal Data by the School

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. However, data may be disclosed to the following third parties without consent:

A. Other schools

If a pupil transfers from either School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress as a result of the move.

B. Examination authorities

This will be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

C. Health authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health, or in case of emergency for the effective treatment of an illness or injury.

D. Police and Courts

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

E. Social workers and Support Agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

F. Educational division

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

G. Right to be Forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

CCTV Cameras

See separate CCTV Policy

Photographs and Videos

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils (aside from a parent recording their own child) during such activities without prior consent.

Keeping in Touch and Supporting the School

The school will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the school may also:

- Share personal data about parents and/or alumni, as appropriate, with our linked charity (Wrekin College Foundation) set up to help establish and maintain relationships with the school community;
- Contact parents and/or alumni (including via the organisations above) by post and email in order to promote and raise funds for the school and, where appropriate, other worthy causes; and/or
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the school's fundraising potential.

Should you wish to limit or object to any such use, or would like further information about them, please contact our DPO (Dr Guy Roberts) in writing.

Whose Rights

- The rights under the Act belong to the individual to whom the data relates. However, the school will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.
- In general, the school will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.
- However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school will maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the pupil or other pupils. Pupils are required to respect the personal data and privacy of others, and to comply with the school's guidelines on pupils' use of ICT, mobile phones and other electronic devices as contained in the school's E-Safety and Online Safety Policies and Acceptable Use Agreement and the School Rules.

Location of Information and Data

- Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored in the school's medical offices.
- All electronic data are stored securely on the school systems, which mainly include the management information system (iSams), CPOMS, RS Admissions, PASS Finance) and Google Drive. The majority of these systems are cloud-based storage systems, with automatic backing-up, accessing and restoring procedures for all data (including off-site backups). The school is aware that data held in remote and cloud storage still requires protection in line with the Data Protection Act. The school will ensure it is satisfied with controls put in place by remote/cloud-based data services providers to protect the data.
- Sensitive or personal information and data should not be removed from the school site. However, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information must not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- The school ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users are assigned a clearance that determines which files are accessible to them. Access to protected data is controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left on accessible/shared printers or photocopiers.

- If information is being viewed on a computer or other device, staff must ensure that the software and documents are properly shut down/logged off and the computer or other device is logged off/locked before leaving it unattended. Any device that can be used to access data should be set to auto-lock if not used for five minutes.
- All users must use strong passwords, which must be changed regularly. User passwords must never be shared.
- Sensitive information must not be viewed on public computers or on any device in a public area (including in a classroom).
- When using home devices or computers to access cloud-based information, they should be password protected and not left unattended whilst logged on. Personal data should not be stored locally on these machines.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - The export of data should have specific approval from the Head
    - The data must be encrypted and password-protected
    - The device must be password-protected
    - The device must offer approved virus and malware checking software
    - The data must be securely deleted from the device, in line with school policy (see Data Disposal, below) once it has been transferred or its use is complete.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care over computers or removable devices which contain personal data; they must NOT be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required for use by an authorised user outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have direct secure remote access to the management information system or other data sources.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if they have specific permission to do so by the Head, and if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf The school has identified a qualified source for disposal of IT assets and collections.

The school also uses shredders to dispose of sensitive printed data.

DBS Certificates

Storage and Access

Certificate information will be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Disposal

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

Research

In the conduct of any research identifying individual children, a member of staff shall ensure that the child or young person's rights are upheld and their privacy respected and shall consult the child and obtain the child or young person's consent to research activity and the publication of any material directly or indirectly identifying the child.

The above is particularly important given that PGCE students may be on placement at any given time at the school.

Pupil Information and Child Protection

The school follows Telford & Wrekin Child Services guidance regarding storage & retention of safeguarding data. https://telfordcs.trixonline.co.uk/chapter/childrens-services-retention-of-records

All child protection records are clearly marked as such and are kept securely locked on the premises or electronically via CPOMS (since September 2021).

Details for recording and sharing of information, transfer, retention, archiving and safe destruction of pupil records is found in the school's Safeguarding and Child Protection Policy and within Telford & Wrekin Child Services guidance on data storage retention.
The schools' procedures are in line with statutory guidance including the Data Protection Act 2018, KCSIE

September 2022 and Working Together to Safeguard Children July 2018.

Queries and Complaints

- Any comments or queries on this policy should be directed to the respective Headteachers using the contact details shown on page 6.
- If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school's complaints procedure and should also notify the above. They can also lodge a complaint with the Information Commissioner's Office (ICO).