Whole School Privacy Policy

This policy should be read in conjunction with the School's **'Staff Code of Conduct'**, '**Whole School Reputation Management and Branding Policy', 'Whole School Data Retention Policy',** and individual **'Privacy Notices'.**

This policy has been prepared with respect and regard to:
The Data Protection Act 2018

Policy Statement:

Cranford School is committed to the protection of all personal and sensitive data collected about past and present staff, pupils, parents, guardians, Governors, visitors and other individuals for which it holds responsibility as the Data Controller, is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and associated legislation and guidelines.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The School is committed to ensuring that all of its staff are aware of data protection policies, legal requirements and that adequate training is provided to them. 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. Any breach of this policy may result in disciplinary action and/or the termination of your contract with the School without notice or compensation.

This policy is non-contractual, although you do have an obligation to comply with its terms. We may amend it from time to time.

This policy meets the requirements of the GDPR and is based on guidance published by the Information Commissioner's Office (ICO). It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Roles and Responsibilities:

The School's Data Protection Officer (DPO) is Mr Steven Wike and is contactable via the School Office. The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The Governing Body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;

- Informing the School of any changes to their personal data, such as a change of address;
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - If there has been a data breach;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they need help with any contracts or sharing personal data with third parties;
    - If anybody raises any queries, concerns or requests relating to their personal data (including invoking the rights referred to below).

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 ICO and, in certain circumstances, to the individual(s) concerned.

Personal and Special Category Data:

All data within the School's control shall be identified as personal or special category 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.

Personal data is defined as any information relating to an identified, or identifiable, individual. This may include the individual's:

- Name and contact details;
- Educational related records, including information about special educational needs and examination results;
- Employment related records, including information about salary and performance;
- Images, audio and video recordings;
- Financial information.

Special categories of personal data are defined as personal data which is more sensitive and so needs more protection. This may include 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. The School only processes such personal data when strictly necessary.

Principles of Data Protection:

The principles of the data protection shall be applied to all data processed. The School will ensure that data is:

- fairly and lawfully processed and in a transparent manner;
- only obtained for lawful purposes and is not further used in any manner incompatible with those original purposes;
- adequately processed, and is relevant and not excessive in relation to the purposes for which it is processed;
- accurate and kept up to date
- not kept longer than is necessary for those purposes;
- kept secure, protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- not transferred to other countries or territories outside the European Economic Areas unless that country or territory ensures an adequate level of protection of the personal information.

Fair Processing and Privacy Notices:

The School will only process data where we have one of 6 'lawful bases' to do so under the GDPR. The lawful bases are:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract;
- The data needs to be processed so that the school can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life;
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions;
- The data needs to be processed for the legitimate interests of the School or a third party (provided the individual's rights and freedoms are not overridden);
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR.

The School will be transparent about the intended processing of data collected and communicate these intentions via the Privacy Notice to staff, parents and pupils prior to the first collection of individual's data.

Limitation, Minimisation and Accuracy:

We will only collect personal data for specified explicit and legitimate reasons. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's **'Whole School Data Retention Policy'**.

Third Parties:

The School will not normally share personal data with anyone else, but there may be circumstances where the School is required either by law or in the best interests of our pupils or staff or in the School's legitimate interests to pass information onto third parties and external authorities such as:

- local authorities;
- independent school bodies such as the Independent Schools Inspectorate (ISI) or the Independent Schools Council (ISC);
- the Department of Health or other health professionals;
- law enforcement and government bodies;
- emergency services;
- visiting peripatetic teachers;
- the School's professional advisers;
- suppliers or contractors who provide services to our staff or pupils, such as IT companies.

We will only share data with a third party that is required to perform the service they have been employed to provide.

These authorities and individuals will be required to demonstrate that they are up to date with data protection law and have their own policies relating to the protection of any data that they receive and process. Examples of data processing activities include:

- enabling the relevant authorities to monitor the School's performance;
- compiling statistical information (normally used on an anonymous basis);
- securing funding for the School (and, where relevant, on behalf of individual pupils);
- safeguarding pupils' welfare and providing appropriate pastoral (and, where relevant, medical and dental) care for pupils;
- where specifically requested by pupils and/or their parents or guardians;
- where necessary in connection with learning and extra-curricular activities undertaken by pupils;
- enabling pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- obtaining appropriate professional advice and insurance for the School;
- where a reference or other information about a pupil or former pupil is requested by another educational establishment or employer to whom they have applied;
- where otherwise required by law; and
- otherwise, where reasonably necessary for the operation of the School.

Further details of anticipated potential third party recipients are available from the School on request.

With the consent of the individual, the School may also share personal data (about former pupils) with any association, society or club set up to establish or maintain relationships with alumni of the School who may contact alumni from time to time by post and/or email about the School and its activities, and for promotional and marketing purposes of the School.

With the consent of the individual, the School may also use their contact details to send promotional and marketing information about the School by post and/or email. However, this will not be shared with any other parties.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the School disclose information or data:

- That would cause serious harm to the individual 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 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 or redacted;
- In the form of a reference given to another school or any place of education and training, the individual's potential employer, or any national body concerned with pupil admissions.

Subject Access Requests:

All individuals whose data is held by the School have a legal right to request access to such data or information about that data. Subject access requests must be submitted in writing to the DPO. They should include:

- Name of individual;
- Correspondence address;
- Contact number and email address;
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

Personal data about a child belongs to that child and not to the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their express permission. This will be assessed on a case-by-case basis and a judgement will be made as to the child's ability to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

When responding to a subject access request we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and normally within 1 month of receipt of the request;
- Will normally provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Is contained in adoption or parental order records;
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the Individual:

In addition to the right to make a subject access request, and to receive information when the School is collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Prevent processing that is likely to cause damage or distress;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

CCTV:

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr Mike Patrick (Network Director). Please also refer to the School's '**CCTV Policy Statement'**.

Photographs and Video:

Images of individuals may be captured at appropriate times and as part of educational activities for use in School only. Uses may include:

- Within School on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of School by external agencies such as the school photographer, newspapers, campaigns;
- Online on our School website or social media pages.

Unless prior consent from parents has been given, the School will not use such images for publication or communication to external sources.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it any new publications.

External parties, including parents, are reminded to ensure that they only take photographs of their own child, for example during performances or at Sports Day and refrain from uploading photographs or videos containing other children to social media sites such as Facebook.

Location of Information and Data:

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Hard copy data, records and personal information are stored out of sight and in a locked cupboard/cabinet. Papers containing confidential personal data must not be left on office and classroom desks where there is general access. The only exception to this is medical information that may require immediate access during the school day. This is stored in a medical filing cabinet in Sick Bay.

Staff should not remove sensitive or personal information and data from the School site, however it is acknowledged that some staff may need to transport data between the School and their home in order to access it for work outside of school hours. This may also apply where staff have off-site meetings or are working between the main School site and the Pre-School site. The following guidelines are provided to staff to assist them in keeping data and information secure and reduce the risk of personal date being compromised:

- Information regarding an individual should not be passed by phone, email, letter, discussion etc. to any person, including parents, unless you are absolutely sure that it is acceptable to do so. If in any doubt, ask the Headmaster or a member of the Senior Leadership Team;
- Paper copies of data or personal information should not be taken off the School site unless absolutely necessary. If these are misplaced, they are easily accessed. If there is no way to avoid taking this information out of School, it should not be on view in public places, or left unattended under any circumstances;
- Round robin emails should be avoided to ensure that viewing the information contained within them is limited to those who need to know about it;
- Ensure that any personal data stored on a PC is deleted when longer required;
- Avoid the use of USB sticks;
- Staff are informed through the **'Staff Code of Conduct'** to avoid where possible using their personal mobile phones to access work emails. At a minimum, ensure that such mobile phones have a password to secure access;
- Avoid discussing individuals in a public place (e.g. Dining Room or corridor);
- Ensure that any documents which contain any personal data on you, staff, parents, pupils or the School, which is not available in the public domain, is shredded or safety disposed of through the School's disposal of sensitive material procedures. Do not throw away into the general rubbish. This also applies to handwritten notes if the notes reference any other staff member or pupil/parent by name. Ensure that pupils are aware that they should be doing the same;
- The School has a 'clear desk policy' and staff are asked to ensure that any documents which contain information of a sensitive or personal nature are not left out for others to view, particularly once they have left for the day;
- Care must be taken to ensure that any printouts of any personal or sensitive information are not left out on desks or left on printer trays or photocopiers;
- Where information is being viewed on a PC screen, staff must ensure that the computer is locked when moving away from the desk at any time. Sensitive information should not be viewed on public computers;
- In the event that sensitive data and information is mislaid, particularly off site, staff must inform the Data Protection Officer;

- Beware of sending defamatory information (slanderous or libellous), for example through posting on social media sites such as Facebook or Twitter. If you comment on or share such comments, you could be sued. The School is also liable if it was conducted using School equipment. Staff are directed to the School's '**Whole School Reputation Management and Branding Policy'** and **'Staff Code of Conduct'** for more details.

These guidelines are clearly communicated to all School staff who sign a '**Data Protection Compliance Form'** (see page 9 of this document) on an annual basis to acknowledge receipt and understanding of the '**Whole School Privacy Policy'**. Any person who is found to be intentionally breaching this will be disciplined in line with the seriousness of their misconduct.

Data Security:

Security of data will be achieved by the implementation of proportionate physical and technical measures. Nominated staff are 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 these organisations must provide evidence of the competence in the security of shared data.

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

Data and information are retained for specific time periods as laid out in the School's '**Whole School Data Retention Policy'.**

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections. Details can be found here**:** http://www.prmgreentech.com/

Personal Data Breaches:

The School will make all reasonable endeavours to ensure that there are no personal data breaches. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a School context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a School laptop containing non-encrypted personal data about pupils

The School has the right to deviate from its policies as it sees fit.

Reviewed: May 2025

Review Due: May 2026

Data Protection Compliance Form

All staff to sign and return to HR on an annual basis. All new staff to sign and return as part of their Induction Programme.

I confirm that I have read and understood the School's **'Whole School Privacy Policy'** ('the Policy') set out in the policies in the Staff Section of the Virtual Learning Environment (VLE) and the **'Privacy Notice for the School Workforce'** ('Privacy Notice').

I acknowledge that the Policy and the Privacy Notice sets out the types of personal data which the School may hold relating to me, the purposes for which such data will be held or processed, the circumstances in which such data may be disclosed and my rights.

I confirm that I have understood my obligations under the Policy and, in particular, with regard to the storage of data pertinent to Cranford School stored off-site at any time and that I am accountable and responsible for its security.

I understand that I have an obligation to immediately report to the School's Data Protection Officer if any information is stolen or mislaid.

…….
Printed Name

…….
Signed

……
Dated