GDPR Policy
St. Crispin's School Leicester Ltd.
2025-2026

This procedure is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
C Lofthouse	
Date of next review	Spring 2026

Key staff involved in the procedure

Role	Name(s)
Head of centre	Andrew Atkin
Senior leader(s)	Chris Lofthouse
Exams officer	Catherine Lofthouse
ALS lead/SENCo	Kerry Massey

General Statement

All school policies are available for parents and prospective parents by contacting St Crispin's School Office on 0116 2707648 or by emailing: enquiries@stcrispins.co.uk

These policies are adapted to cover the whole school from 2-16 and therefore this policy applies to the whole school, including the EYFS. It should be read by parents/staff alongside all the school policies, the School Welcome Pack and the Admission Form and for staff additional information can be found in the St. Crispin's Staff Handbook and their Terms and Conditions of Employment. St Crispin's School is committed to safeguarding and promoting the welfare of pupils and young people and expects all staff and volunteers to share this commitment. It is our aim that all pupils fulfil their potential.

The parents of the children attending St Crispin's School should be aware that the school has a duty to safeguard and promote the welfare of children who are their pupils. This responsibility necessitates a Safeguarding Policy and School may need to share information and work in partnership with other agencies when there are concerns about a child's welfare.

Policy Statement

We outline all the action that we have taken to protect data and privacy within the school and its external systems.

Aims and Objectives

This attendance policy ensures that all staff in our school are fully aware of and clear about the actions necessary to protect data and privacy.

Policies

- Data Protection subject access.
- Data retention and breach escalation.
- Privacy Policy.
- Privacy notices.
- Data Protection Officer. CAL
- E Safety Policy.

Equipment

- Shredder
- Encrypted Data HDD

School

- Regular removal of old data.
- CCTV
- Recycling of old data equipment.

IT

- Regularly check n Drive privileges.
- Penetration tests undertaken.
- Installation and updates of Ransomware.
- Subject access check.
- Privacy impact access check.
- Removal of 3rd Party processes.
- USB restrictions.
- Breach escalation processes in place. (Reporting to GDPR)
- Alert regulator within 72 hours.

Staff

- Data handling training.
- Refresher courses.

Hub

- Security Testing.
- Delete old data.
- Subject access restrictions.
- Ensure data portability.
- Privacy by design.
- Regular restoration of data.
- All information moved to a onsite server.
- Curriculum plan in place to ensure correct data displayed.

Data Protection

- Establish legal basis with staff and parents (Terms and Conditions).
- Consent freely given.
- Records kept of consent.
- To be able to withdraw consent.
- Can request to delete data.
- Can request all data.
- Data encrypted.