



STAFF CODE OF CONDUCT

Written by: RS	September 2025
Current version no: 1	
Reviewed:	September 2025
Approved by the Governing Body:	September 2025
Next review:	September 2026

Taking and Storing Images of Children Policy

1. Policy Statement

This Policy provides information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Sancton Wood School ("the School"). It sets out the School's commitment to protecting pupils through the safe and appropriate use of photography, video recording, and digital imaging.

This policy applies in addition to the School's Terms and Conditions, Safeguarding and Child Protection Policy, Data Protection Policy, Online Safety Policy, Anti-Bullying Policy, and any other relevant school policies.

Safeguarding Context: The inappropriate use, sharing, or storage of images can pose significant safeguarding risks to children, including potential for peer-on-peer abuse, exploitation, and online harm. This policy is designed to prevent such risks while enabling the positive use of images to celebrate achievements and promote the school.

2. Legal Framework and Data Protection

2.1 Legal Basis for Processing

The School processes images of pupils under the following legal bases:

- **Legitimate interests** (Article 6(1)(f) GDPR) for routine school operations, safety, and promotional activities



- **Consent** (Article 6(1)(a) GDPR) for external marketing and media use
- **Legal obligation** (Article 6(1)(c) GDPR) for identification and security purposes
- **Public task** (Article 6(1)(e) GDPR) for educational activities

2.2 Individual Rights

Parents and pupils (aged 12+) have the right to:

- **Access** copies of images held by the school
- **Object** to processing for legitimate interests
- **Withdraw consent** where processing is based on consent
- **Request deletion** where there is no overriding legitimate interest
- **Data portability** for images held with consent

2.3 Data Retention

- **Educational images:** Retained for the duration of the pupil's education plus 7 years
- **Marketing images:** Retained for 7 years or until consent is withdrawn
- **Security/ID images:** Retained for 7 years after leaving school
- **CCTV images:** Retained according to CCTV Policy, 31 days.

3. Consent and Decision-Making

3.1 Consent Process

Parents accepting a place for their child will be asked to complete a comprehensive consent form covering:

- Internal school displays and communications
- Website and social media use
- External marketing and promotional materials
- Media photography and filming
- Professional photography sessions

3.2 Pupil Voice and Conflicting Decisions

Recognising that children aged 12+ have their own data protection rights:

- **If a pupil objects** to image use, it will not proceed even if parents have consented
- **If parents object but pupil (Year 7+) consents**, images will not be used to avoid reputational damage
- **If pupil is under 12**, parents' decision will generally take precedence
- All decisions will be recorded and staff informed via the permissions database



3.3 Ongoing Consent Management

- Consent can be withdrawn at any time by notifying the school in writing
- The Communications Lead (Ioana Bird) maintains the current permissions database
- Staff must check permissions before any image use
- Regular consent reviews will be conducted annually

4. Safeguarding Requirements

4.1 Preventing Peer-on-Peer Abuse

The School recognises that images can be used to facilitate peer-on-peer abuse, including:

- **Sexual harassment** through inappropriate sharing or commentary
- **Bullying and humiliation** through unflattering or embarrassing images
- **Exploitation** through manipulation or coercion
- **"Sexting"** and inappropriate intimate images

4.2 Online Safety and Digital Risks

In line with KCSIE 2025, the School addresses online safety risks including:

- **Misinformation and disinformation** using manipulated images
- **Conspiracy theories** spread through fake imagery
- **Inappropriate sharing** on social media platforms
- **Contact from strangers** through publicly available images

4.3 Staff Safeguarding Responsibilities

All staff must:

- Complete annual safeguarding training including appropriate image use
- Report concerns about image misuse immediately to the DSL
- Follow the School's Code of Conduct regarding photography
- Understand the risks of inappropriate image sharing

5. Taking Photographs and Videos

5.1 Staff Guidelines

Staff must not take photographs or videos that:

- Might cause embarrassment, distress, or humiliation



- Are associated with sensitive or distressing situations
- Are taken during one-to-one situations without clear educational justification
- Are unnecessarily intrusive or inappropriate
- Could be misinterpreted or misused

5.2 Appropriate Photography

Acceptable photography includes:

- Celebrating achievements and school events
- Educational activities and learning outcomes
- Sports and extra-curricular activities
- Marketing and promotional activities (with consent)
- Official school documentation

5.3 Device Requirements

Preferred Practice:

- Staff should use School-owned devices and cameras
- Contact the front office for School devices or Marketing Department for cameras

Personal Device Use (when School devices unavailable):

- Images must be transferred to School network immediately
- Images must be deleted from personal devices after transfer
- No uploading to personal computers without prior authorisation
- Strict prohibition on personal social media posting
- Full compliance with Staff ICT Acceptable Use Policy required

6. Use of Pupil Images

6.1 Internal School Use

Unless specifically restricted, images may be used for:

- Internal displays on digital and conventional notice boards
- Communications with school community (email, internal systems, post)
- Educational purposes and classroom activities
- Administrative functions and record keeping



6.2 External and Online Use

With appropriate consent, images may be used for:

- School website and official social media channels
- Prospectus and marketing materials
- Press and media coverage
- Professional promotional photography

Safety Measures:

- External images will not include pupils' full names
- No personal information disclosed beyond first name and year group
- Images selected to be appropriate and respectful
- Regular review of online content

6.3 Identification and Security

Mandatory Uses:

- Annual identification photographs (filed by admission number only)
- CCTV recording for security purposes
- Educational visits and off-site activity registers

7. Media and Professional Photography

7.1 Media Visits

- Parents notified in advance of expected media attendance
- Pupils without permission protected from photography/filming
- Media accompanied by staff member at all times
- Names provided only with explicit consent
- Right to refuse participation protected

7.2 Professional Photographers

- All photographers must be accompanied unless full DBS-checked
- Clear instructions provided regarding consent restrictions
- Secure storage and handling requirements specified
- Images held responsibly and according to school instructions
- Contract includes data protection and security clauses



8. Parent and Family Photography

8.1 Guidelines for Parents

Parents may photograph their own children at school events subject to:

- **Respect for others:** No photographing other children without parental consent
- **Personal use only:** Images must not be shared publicly or posted online
- **Privacy protection:** No photography in changing rooms, toilets, or backstage areas
- **Copyright respect:** Adherence to restrictions on plays and concerts
- **School authority:** Following specific event guidance and restrictions

8.2 Enforcement

The School reserves the right to:

- Refuse or withdraw photography permission from non-compliant parents
- Request deletion of inappropriately taken images
- Remove individuals who breach guidelines
- Report serious breaches to appropriate authorities

9. Pupil Use of Cameras and Mobile Devices

9.1 Acceptable Use

- Educational photography with teacher permission
- Celebrating appropriate school activities and achievements
- Following school rules and acceptable use policies
- Respecting others' privacy and dignity

9.2 Prohibited Use

- Photography in toilets, changing rooms, or private areas
- Taking images that might cause embarrassment or upset
- Sharing inappropriate or intimate images ("sexting")
- Using images for bullying, harassment, or humiliation
- Posting images of others without permission

9.3 Reporting and Support

Pupils are encouraged to:

- Report concerning use of cameras or images immediately



- Seek help if pressured to share inappropriate images
- Support peers who may be experiencing image-related abuse
- Understand the serious consequences of image misuse

10. Security and Technical Safeguards

10.1 Storage Security

- Images stored on secure school network systems
- Access restricted to authorized staff with legitimate need
- Regular backup and recovery procedures
- Encryption for any portable storage devices
- Secure deletion procedures for end-of-life storage

10.2 Access Controls

- Role-based access to image databases
- Activity logging for image access and use
- Regular access reviews and permission updates
- Password protection for all image storage systems
- Separation of different types of image use

10.3 Transfer and Sharing

- Secure file transfer protocols for external sharing
- Written agreements for third-party image handling
- Clear restrictions on further use or distribution
- Audit trail for all image transfers
- Immediate reporting of any data breaches

11. Incident Response and Safeguarding Concerns

11.1 Types of Incidents

Immediate DSL notification required for:

- Inappropriate sharing of pupil images
- Suspected peer-on-peer abuse involving images
- Unauthorized photography or filming
- Potential "sexting" incidents
- External requests for pupil images
- Data breaches involving pupil images



11.2 Response Procedures

Immediate Actions:

1. Secure any evidence (devices, images, communications)
2. Notify Designated Safeguarding Lead immediately
3. Document all known facts without questioning children
4. Separate individuals involved if necessary
5. Preserve confidentiality pending investigation

Follow-up Actions:

- Risk assessment for pupil safety and wellbeing
- Parent/carers notification as appropriate
- Police involvement if potential criminal activity
- Support for affected pupils
- Review and improvement of procedures

11.3 Support and Education

Following incidents:

- Individual support for affected pupils
- Targeted education on appropriate image use
- Review of supervision and monitoring procedures
- Updates to policies and training as required

12. Training and Awareness

12.1 Staff Training

All staff receive training on:

- Appropriate use of cameras and image capture
- Recognising signs of image-related abuse
- Data protection and consent requirements
- Incident reporting and response procedures
- Online safety and digital citizenship

12.2 Pupil Education

Through PSHE and computing curricula:



- Understanding consent and privacy rights
- Recognising inappropriate image requests
- Consequences of image misuse
- Seeking help and reporting concerns
- Digital citizenship and online safety

12.3 Parent Information

Regular communication about:

- School image use policies and procedures
- Home online safety guidance
- Recognising concerning behaviours
- Supporting children's digital wellbeing

13. Monitoring and Review

13.1 Policy Review

- Annual review by Senior Leadership Team
- Incorporation of new guidance and legislation
- Analysis of incidents and lessons learned
- Updates to reflect technological changes
- Consultation with school community as appropriate

13.2 Compliance Monitoring

- Regular audits of image storage and access
- Review of consent records and permissions
- Assessment of staff compliance with procedures
- Evaluation of incident response effectiveness
- External review as part of safeguarding audits

14. Related Policies and Guidance

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Data Protection and Privacy Policy
- Online Safety Policy
- Anti-Bullying Policy
- Behaviour Policy



- Staff Code of Conduct
- Acceptable Use Policies (Staff and Pupils)
- CCTV Policy

15. Contacts and Further Information

For image permission queries: Communications Lead (Ioana Bird)

For safeguarding concerns: Designated Safeguarding Lead

For data protection queries: Data Protection Officer

Emergency concerns: Head Teacher or Deputy Head Teacher

External Contacts:

- Local Authority Designated Officer (LADO): 01223 727 967
- Cambridgeshire Children's Services: 0345 045 0180
- Police (non-emergency): 101
- Police (emergency): 999