

St. Gerard's
School & Support Services



Acceptable Use of ICT Policy

Purpose

This policy sets out how **ICT resources are to be used safely, professionally and responsibly within St Gerard's School & Support Services**, across both the **Balmoral and Suffolk sites**.

ICT systems are provided to:

- Support teaching, learning and assessment;
- Enable effective communication with pupils, parents, staff, governors and external agencies;
- Protect sensitive pupil, family and staff information;
- Ensure compliance with **EA, CCMS, GDPR and safeguarding requirements**.

Misuse of ICT may put pupils at risk, compromise safeguarding, damage the reputation of St Gerard's and lead to disciplinary action.

Scope

This policy applies to:

- All teaching and non-teaching staff;
- Classroom assistants, support services staff and volunteers;
- External professionals and contractors accessing ICT systems;
- Any individual authorised to use **EA-provided or school-owned ICT equipment**.

It applies:

- During working hours and outside of hours;
- On school premises and when working remotely;
- When using school-owned devices or **personal devices to access school systems**.

ICT Resources Covered

This policy applies to all ICT resources used within St Gerard's, including:

- Desktop computers, laptops and tablets;
- Interactive screens and classroom technology;
- Mobile phones and smart devices used for work purposes;
- Email systems, internet access and cloud platforms;
- Removable media (USBs, external drives);
- School management information systems and pupil records.

Responsibilities

School Leadership & Management

- The **Principal** has overall responsibility for ensuring this policy is implemented within St Gerard's.
- The **Senior Leadership Team (SLT)** will ensure staff understand and comply with acceptable use standards.
- ICT misuse or safeguarding concerns will be addressed promptly and in line with:
 - EA Disciplinary Procedures
 - Safeguarding and Child Protection procedures

Staff Responsibilities

All staff must:

- Read, understand and comply with this policy;
- Complete required ICT and data protection training;
- Use ICT in a way that safeguards pupils and protects confidential information;
- Report concerns or breaches immediately to a member of SLT.

Safeguarding and Data Protection (School-Specific Emphasis)

Given the nature of St Gerard's provision:

- **Pupil data is highly sensitive** and often relates to medical, behavioural and safeguarding needs.
- ICT must be used with **particular care**, especially when:
 - Communicating about pupils with complex needs;
 - Supporting pupils during regulated or unregulated activities;
 - Sharing information with multi-agency partners (e.g. AHPs, EA, CAMHS).

Staff must ensure:

- Pupil information is shared **only on a need-to-know basis**;
- Emails containing personal or sensitive data are encrypted where required;
- Screens are not visible to unauthorised persons;
- Printed materials are stored securely and disposed of appropriately.

Email and Digital Communication

Staff must:

- Use **school/EA email accounts only** for school business;
- Communicate professionally and respectfully at all times;
- Assume emails may be disclosed in inspections, complaints or legal proceedings;
- Report any inappropriate or offensive material received immediately.

Staff must **not**:

- Use personal email or messaging apps (e.g. WhatsApp) for professional communication with parents or pupils unless explicitly authorised by the school;
- Forward pupil or staff data without appropriate safeguards;
- Auto-forward school emails to personal accounts.

Internet and Social Media Use

Internet access at St Gerard's is filtered and monitored.

Staff must:

- Use the internet to support teaching, learning and professional duties;
- Follow the **St Gerard's Social Media and Communications Policy**;
- Never comment publicly on pupils, families or school matters.

Staff must **not**:

- Access inappropriate or unsafe material;
- Use proxy or bypass systems;
- Make personal use of social media that could bring the school into disrepute.

Mobile Computing and Personal Devices

Mobile devices are widely used to support learning and communication at St Gerard's. Staff must:

- Keep devices secure at all times;
- Use passwords and encryption where required;
- Screen-lock devices when not in use;
- Report lost or stolen devices immediately.

Staff must **not**:

- Store pupil data on personal devices without authorisation;
- Photograph pupils on personal devices unless approved and in line with consent;
- Use unsecured public Wi-Fi for accessing school systems.

Removable Media (USBs etc.)

Staff must:

- Use only **EA-approved removable media**;
- Ensure data is encrypted and minimised;
- Return or securely erase media when no longer required.

Use of personal USB devices is **not permitted**.

Monitoring and Privacy

Use of ICT systems within St Gerard's:

- Is monitored in line with EA policy and legislation;
- May be reviewed where safeguarding, security or disciplinary concerns arise.

Monitoring will always be:

- Proportionate;
- Authorised;
- Carried out in accordance with legal requirements.

Breaches and Disciplinary Action

Failure to comply with this policy may result in:

- Withdrawal of ICT access;
- Disciplinary action under EA procedures;
- Referral to external agencies where required (e.g. PSNI, Social Services).

Safeguarding-related breaches will always be treated as a **serious matter**.

Review

This policy will be:

- Reviewed regularly by **SLT and Governors**;
- Updated in line with EA guidance, safeguarding requirements and technological developments.