

DIGITAL & DATA HANDLING POLICY

Applicable to:	RGS Guildford RGS Prep, including EYFS
Author(s):	Director of IT
Executive owner:	Deputy Head Director of Finance & Operations
Date of last review:	July 2026
Date of next review:	Trinity 2027

Contents

1. Purpose and scope	4
2. Principles and values	6
2.1 Safety first	6
2.2 Technology in service of education	6
2.3 Clarity and consistency	6
2.4 Inclusion and equity	6
2.5 Privacy, security and accountability	6
2.6 Proportionate innovation	6
2.7 Phase-appropriate practice	6
3. Roles and responsibilities	7
3.1 Governing Board	7
3.2 Headmaster, Head of Prep and senior leaders	7
3.3 Designated Safeguarding Leads and deputies	7
3.4 Director of IT and IT Services	7
3.5 Data Protection Officer and data governance leads	8
3.6 Exams Officer and assessment leaders	8
3.7 Heads of Department, pastoral leaders and middle leaders	8
3.8 Teaching and support staff	9
3.9 Students	9
3.10 Parents and carers	9
4. Online safety and digital safeguarding	10
4.1 Whole-School approach	10
4.2 Age-appropriate practice across Prep and Senior	10
4.3 Filtering, monitoring and technical safeguards	10
4.4 Classroom monitoring and digital supervision	11

4.5 Reporting concerns.....	11
4.6 Digital conduct and safeguarding overlap.....	11
4.7 Remote learning and communication	12
5. Digital teaching, learning and innovation	13
5.1 Educational purpose	13
5.2 Phase-appropriate expectations.....	13
5.3 Inclusion, access and reasonable adjustment.....	13
5.4 Emerging tools and professional judgement	13
5.5 Staff development and leadership	14
6. 1-1 Device arrangements	15
6.1 General approach.....	15
6.2 Phase-specific arrangements	15
6.3 Digital Levy and School-managed devices.....	15
6.4 Daily readiness and care of devices.....	15
6.5 Use in lessons and for homework	16
6.6 Restrictions, software and technical control	16
6.7 Hotspots, VPNs and alternative connections.....	16
6.8 Home use and parental oversight	16
6.9 Device issues, faults and support.....	17
7. Acceptable use and digital conduct	18
7.1 General principles	18
7.2 Staff acceptable use and digital conduct	18
7.3 Student acceptable use and digital conduct: RGS Prep	19
7.4 Student acceptable use and digital conduct: RGSG Senior School	20
7.5 Conduct beyond the School site	20
7.6 Sanctions, support and restoration.....	21
8. Data handling, account security and records.....	22
8.1 General expectations	22
8.2 Use of School systems for School data	22
8.3 Special category and higher-risk data.....	22
8.4 Account security.....	22
8.5 Monitoring, logging and investigation	23
8.6 Data breaches and incidents	23
8.7 Records, retention and continuity	23
8.8 Leavers, transfers and access changes	23

8.9 Further detail.....	24
9. Emerging tools and services	25
9.1 Approach.....	25
9.2 Approval before use and adoption	25
9.3 Review criteria	25
9.4 Generative and adaptive tools	25
9.5 No assumption of entitlement	26
9.6 Review and withdrawal	26
10. Assurance, monitoring and review	27
10.1 Governance and assurance	27
10.2 Monitoring implementation.....	27
10.3 Policy review.....	27
11. Communication and training	28
11.1 Communication.....	28
11.2 Staff training and induction.....	28
11.3 Student education	28
12. Digital operations, support and printing	29

1. Purpose and scope

The Royal Grammar School, Guildford and RGS Prep (together, “the School”) are committed to providing the highest standard of education and pastoral care. This policy reflects the School’s values, ensuring clarity and consistency for pupils, staff and parents.

Throughout this policy, the terms ‘child’, ‘pupil’ or student’ are used to refer to all those attending the School. At the time of publication, the School is a boys’ School but is preparing to become co-educational. Nursery, Reception (Shell) and Year 3 at RGS Prep, and Year 12 (Lower Sixth) at RGS Senior will become co-educational from September 2027. Year 7 (1st Form) at RGS Senior will become co-educational from September 2028.

This policy sets out how Royal Grammar School, Guildford (RGSG) and RGS Prep use and govern digital systems, devices, data and online services across teaching, learning, safeguarding, administration and assessment.

It provides the School’s overarching framework for:

- online safety and digital safeguarding;
- digital teaching, learning and innovation;
- the use of School devices and services, including the Microsoft 365 environment and the Device programme;
- acceptable use and digital conduct by staff and students;
- data handling, account security and records;
- the governance of emerging digital tools, including generative technologies.

This policy applies to both RGSG and RGS Prep. It applies to governors, employees, temporary staff, volunteers, contractors, visitors, students and, where relevant, parents and carers when they engage with School digital systems, School data or School-managed devices.

This is a whole-School policy. It does not replace specialist statutory or operational policies. It should be read alongside, in particular, the following policies:

Prep:

- Behaviour, Rewards and Discipline Policy

Senior:

- Behaviour (Rewards and Sanctions) Policy
- Exams Policy
- Exam Malpractice and AI Policy

Whole School:

- Account Security and Monitoring Policy
- Information and Records Retention Policy
- Privacy Notice (Parents)
- Privacy Notice (Staff)
- Privacy Notice (Students aged 13+)
- Privacy Notice

- Safeguarding Policy
- SEND Policy
- Staff Data Handling and Device Use Policy

Where a matter concerns immediate safeguarding, allegations against staff, a personal data breach, or suspected examination malpractice, the relevant specialist policy or procedure takes precedence and must be followed without delay.

2. Principles and values

The School's approach to digital and data is guided by the following principles.

2.1 Safety first

The welfare of children is paramount. Digital systems, devices and online services must be used in ways that safeguard students, reduce foreseeable risk and support a culture in which concerns are identified and acted on promptly.

2.2 Technology in service of education

The School embraces digital tools as powerful enablers of teaching, learning, inclusion, organisation and communication. All digital practice should be purposeful and proportionate, guided by sound educational judgement to ensure technology consistently adds value and enriches the experience of every learner.

2.3 Clarity and consistency

Staff, students and parents should be able to understand what is expected, what is permitted, what is not permitted, and what will happen if things go wrong. The School will therefore aim to keep expectations clear, practical and consistent across its systems and policies.

2.4 Inclusion and equity

Digital provision must support access, participation and fairness for students across both Schools, including students with SEND or other needs that affect how they learn, record work or access School systems. Where different arrangements are required, these should be planned and documented clearly.

2.5 Privacy, security and accountability

The School handles personal data lawfully, fairly and securely, and expects all members of the School community to do the same. Access to School systems is a professional responsibility, and every user is accountable for the way they use School accounts, devices and data.

2.6 Proportionate innovation

The School recognises that digital services and generative technologies will continue to evolve. New tools may be adopted where they are educationally useful, operationally sound, legally compliant and safe for students and staff. Innovation is encouraged within the guidelines and School structures outlined in this document, supported by an appropriate review and approval process.

2.7 Phase-appropriate practice

The School serves two distinct contexts: RGS Prep and RGSG. Some expectations must therefore differ by age, stage and setting, especially in relation to devices, independence, parental involvement, safeguarding controls and assessment arrangements. Where this policy distinguishes between the Schools, those distinctions are intentional and should be applied consistently.

3. Roles and responsibilities

Clear accountability is essential if this policy is to be workable in practice.

3.1 Governing Board

The Governing Board has strategic oversight of digital and data governance across the School.

In particular, the Governing Board is responsible for ensuring that:

- the School has an appropriate policy framework for digital safeguarding, data protection, cyber security, assessment integrity and acceptable use;
- leaders are held to account for implementation, compliance and review;
- online safety is treated as a whole-School safeguarding issue rather than only a technical matter;
- the School does all that it reasonably can to limit students' exposure to online risks from the School's IT systems; and
- appropriate assurance is received on incidents, trends, training, filtering and monitoring, and the effectiveness of controls.

3.2 Headmaster, Head of Prep and senior leaders

The Headmaster and the Head of Prep, supported by senior leaders, are responsible for the implementation of this policy in day-to-day practice within their respective Schools. This includes ensuring that digital systems, expectations and staff training support safe, effective and educationally sound practice.

Senior leaders are responsible for ensuring that digital and data issues are not treated in isolation. They must be integrated with safeguarding, behaviour, SEND, staff conduct, curriculum, assessment and operational risk management.

3.3 Designated Safeguarding Leads and deputies

The Designated Safeguarding Lead for RGSG and the Designated Safeguarding Lead for RGS Prep are responsible for leadership of online safety and digital safeguarding within their respective Schools, in line with the Safeguarding Policy.

This includes:

- oversight of safeguarding concerns arising from online activity, device use, digital communication, images, filtering or monitoring alerts;
- ensuring that concerns are triaged promptly and appropriate action is taken in line with safeguarding procedures;
- advising on safeguarding implications when digital services, monitoring tools or new technologies are introduced or reviewed; and
- ensuring that online safety education remains coherent, age-appropriate and joined up across curriculum and pastoral provision.

3.4 Director of IT and IT Services

The Director of IT is responsible for the operational management of the School's digital environment, including infrastructure, identity, device management, core services, technical controls and service support.

This includes responsibility for:

- the secure and effective operation of School systems and School-managed devices;
- technical implementation of filtering, monitoring, access controls, device restrictions and other cyber security measures;
- oversight of device deployment and support, including the Device programme and associated service arrangements;
- advising leaders on feasibility, risk and implementation when policy or practice changes are proposed; and
- supporting the evaluation and approval process for new services and applications, alongside safeguarding and data-protection colleagues.

3.5 Data Protection Officer and data governance leads

The Data Protection Officer is responsible for advising the School on data-protection compliance, privacy, subject rights, data breaches, records handling and data-sharing risk.

This includes:

- oversight of personal data breaches and suspected breaches;
- advice on lawful bases, transparency, retention and information rights;
- support for data protection impact assessments and the approval of new services where personal data is involved; and
- advising on the use of generative or third-party tools where personal data, special category data or business-critical data may be involved.

3.6 Exams Officer and assessment leaders

The Exams Officer, together with relevant senior leaders, is responsible for ensuring that the use of digital tools in examinations and formal assessments is compliant with current awarding body and regulatory requirements.

This includes:

- briefing staff and students on malpractice, including misuse of digital and generative tools in assessed work;
- ensuring that arrangements for word processors and other digital support are available for students in line with their normal way of working and any approved access arrangements; and
- escalating suspected malpractice in accordance with the Exams Malpractice Policy.

3.7 Heads of Department, pastoral leaders and middle leaders

Heads of department, pastoral leaders and other middle leaders are responsible for implementing this policy consistently within their area of responsibility. They must ensure that staff and students understand the expectations that apply to classroom practice, homework, communication, conduct and assessment.

They are also responsible for spotting patterns of misuse, inconsistency or avoidable workload, and for raising these so that practice can be improved.

3.8 Teaching and support staff

All staff are responsible for using School systems, devices and data safely, lawfully and professionally. This includes following School rules on accounts, passwords, communications, cloud services, personal devices, monitoring, data handling, images, and the use of emerging digital tools.

All staff must understand that online safety is part of safeguarding, that data protection is part of professional responsibility, and that concerns must be reported promptly through the correct route.

3.9 Students

Students are responsible for using School devices, accounts and digital services safely, respectfully and in line with School expectations. As students mature, the School expects increasing independence, but not at the expense of safety, honesty or good judgement.

Because RGS Prep and RGSG serve students at different stages, the detail of those expectations will differ between the Schools and between age groups. Those differences are set out in the relevant sections of this policy and in the student agreement appendices.

3.10 Parents and carers

Parents and carers play an important supporting role, especially in relation to home use of devices, routines, boundaries, communication with the School and reinforcement of safe online habits.

For Prep students in particular, parental support is an important part of effective device management, age-appropriate supervision and the development of good habits around organisation, screen use and online conduct. For older students, the School will continue to work with parents while recognising that expectations for independent use will increase with age and stage.

4. Online safety and digital safeguarding

4.1 Whole-School approach

The School recognises that online safety is a safeguarding matter and must be treated as part of the School's wider safeguarding culture, systems and practice.

Online safety is therefore not confined to technical controls or isolated curriculum sessions. It includes the education of students, the conduct of staff, the use of School devices and services, the management of digital communication, the handling of incidents, and the way concerns are identified, reported and followed up.

The School will take a whole-School approach to online safety across both RGSG and RGS Prep. This means that safeguarding, pastoral, curriculum, digital and technical leaders must work together so that expectations are clear, age-appropriate and consistently applied.

The School will teach students about online safety in ways that are appropriate to their age, stage and context. This will include, where relevant, online relationships, respectful behaviour, digital reputation, misinformation, inappropriate content, harmful contact, coercion, exploitation, privacy, consent, image-sharing, and the responsible use of emerging digital tools.

4.2 Age-appropriate practice across Prep and Senior

The School recognises that students at RGS Prep and RGSG require different levels of supervision, independence and parental involvement.

At RGS Prep, online safety arrangements will place greater emphasis on adult guidance, structured routines, close supervision, clear boundaries and partnership with parents. Expectations for independent decision-making will be introduced gradually and reinforced consistently.

At RGSG, students will be expected to take increasing responsibility for their conduct, judgement and organisation. This greater independence does not reduce the School's safeguarding responsibilities. Rather, it requires clearer expectations, stronger habits of reporting, and regular reinforcement of safe and responsible behaviour.

Where different arrangements apply to the two Schools, those differences should reflect age and stage, not lower standards.

4.3 Filtering, monitoring and technical safeguards

The School uses filtering, monitoring and other technical safeguards to help reduce students' exposure to harmful or inappropriate material, identify possible risks, support classroom management and protect the School's systems and data.

These safeguards form part of the School's wider safeguarding and security arrangements. No filtering or monitoring system can be relied upon to be 100% effective or accurate at all times, and these systems do not replace professional curiosity, staff supervision, pastoral oversight or the prompt reporting of concerns.

The School may monitor the use of its network, cloud services, accounts and managed devices for safeguarding, security, operational and legal reasons. Monitoring may include web activity, account activity, file activity, email and cloud-service logs, and the use of classroom management tools during School hours or other authorised times.

Access to monitoring systems and related information is restricted to authorised staff and will be used only for legitimate educational, safeguarding, security and operational purposes. Monitoring operates during periods when the School's monitoring arrangements are active and should not be regarded as continuous supervision of a student's online activity. Parents and carers retain primary responsibility for supervising and supporting their child's online activity outside these arrangements. Where an alert, concern or safeguarding issue is identified, the School reserves the right to carry out proportionate further enquiries, including reviewing relevant internet usage records, search history and device activity, where necessary to assess risk, safeguard students or investigate potential breaches of School policies. Relevant information will be shared with parents, carers or external agencies where appropriate and in accordance with safeguarding and data protection requirements.

4.4 Classroom monitoring and digital supervision

Where the School uses classroom monitoring or device-management tools, these must be used only for legitimate educational, pastoral, safeguarding, technical support or examination-related purposes.

Staff must use such tools professionally and proportionately. They must not use them for casual surveillance, personal curiosity or any purpose outside their role.

Any accidental, inappropriate or unauthorised access to student information or screens must be reported immediately through the appropriate safeguarding or data-protection route.

4.5 Reporting concerns

All members of staff must report safeguarding concerns arising from online activity, device use, digital communication, images, monitoring alerts or other digital behaviour in line with the Safeguarding Policy and any relevant internal procedure.

Students must be taught how to report a concern, whether the concern relates to their own experience or to the safety of another student. Reporting routes should be clear, visible and reinforced regularly.

Parents and carers should be able to raise concerns about online safety, device use or digital conduct through the usual School channels. Concerns should be taken seriously and directed promptly to the appropriate member of staff.

If a concern indicates that a child may be at risk of harm, the matter must be treated as a safeguarding concern and escalated without delay.

4.6 Digital conduct and safeguarding overlap

The School recognises that not all poor digital behaviour is a safeguarding matter, but some behaviour may move quickly from a conduct issue to a safeguarding concern.

Staff must therefore exercise judgement and seek advice where needed. This applies in particular to issues involving bullying, harassment, sexualised behaviour, image-sharing, coercion, threatening behaviour, radicalisation concerns, attempts to bypass safeguards, or patterns of behaviour suggesting vulnerability or harm.

Where behaviour may engage both behaviour and safeguarding processes, the School will ensure that those processes are aligned and that the child's welfare remains central.

4.7 Remote learning and communication

Where digital systems are used for remote learning, homework, communication or pastoral support, the same standards of safeguarding, professionalism and clarity apply as in face-to-face settings.

Staff must use approved School systems and communication channels. Students must understand the expectations that apply to behaviour, participation, communication and conduct when engaging online.

Any remote practice involving live communication, shared files, recorded content or digital interaction must be planned and managed in a way that protects students, staff and the integrity of the learning environment as directed by the safeguarding team and outlined in the safeguarding policy.

5. Digital teaching, learning and innovation

5.1 Educational purpose

The School's priority is consistently strong teaching and learning. Digital tools are used where they improve teaching, learning, inclusion, organisation or feedback, not simply because they are available.

The School does not expect uniformity in every classroom. It does, however, expect digital practice to be deliberate, professionally sound and aligned with agreed whole-School expectations.

Digital practice should support learning and enhance attainment. Staff should use professional judgement to decide when digital tools add value, when analogue methods are more effective, and when a blended approach is most appropriate.

5.2 Phase-appropriate expectations

The School recognises that effective digital practice will not look identical in RGS Prep and RGSG.

At RGS Prep, digital practice should emphasise structure, routine, modelling and the gradual development of digital skills, habits and confidence in preparation for Senior School. Younger students should be taught how to use devices and services, but teaching should remain appropriately balanced, with careful attention to screen use, handwriting, oral work and practical activity.

At RGSG, digital practice should support increasing independence, academic organisation, collaborative working and effective preparation for later study. Staff should still apply professional judgement and avoid assumptions that all learning is improved by increased device use.

Across both Schools, the School's expectation is not 'digital first' but 'best method for the learning'.

5.3 Inclusion, access and reasonable adjustment

Digital systems and devices can improve access to learning, but they can also create barriers if used without thought.

Staff must take account of students with SEND and other needs that affect access, organisation, processing, writing, reading, memory, communication or self-regulation. Where digital arrangements support access, those arrangements should be used consistently and coherently.

The School should distinguish clearly between:

- whole-cohort digital routines;
- classroom strategies used at a teacher's discretion; and
- specific access arrangements, support plans or reasonable adjustments for individual students.

This is particularly important where a student's normal way of working may later be relevant to internal assessment or public examinations.

5.4 Emerging tools and professional judgement

The School recognises that emerging digital tools, including generative technologies, may offer useful support in planning, explanation, feedback, accessibility and administration.

Such tools must be used with professional judgement. Staff must not use them in ways that compromise student safety, confidentiality, fairness, assessment integrity or educational quality. Students may use approved digital tools only within the boundaries set by the School, their teachers and the relevant assessment rules. The School will make clear when such use is permitted, when it must be acknowledged, and when it is prohibited.

5.5 Staff development and leadership

The School will support staff to develop confidence and consistency in digital practice through training, shared exemplification, coaching and professional dialogue.

Digital development should be practical and curriculum-facing. It should help staff make better decisions about learning design, organisation, accessibility, assessment and the use of emerging tools.

The School may use designated digital leadership roles, including coaching or coordination functions, to help departments refine practice, spread effective approaches and maintain alignment with whole-School expectations.

6. 1-1 Device arrangements

6.1 General approach

The School provides and manages a structured device environment in order to support teaching, learning and operations, strengthen safeguarding, improve consistency, reduce avoidable technical variation and protect School data.

The device programme and associated digital services form part of the School's educational and operational infrastructure. Device provision is therefore not simply a matter of parental preference or personal convenience.

The School specifies the categories of device permitted for School use, the software and services used alongside them, and the technical controls required to support safeguarding, access and reliability. This is reviewed periodically to ensure that devices and software remain appropriate for the age, developmental needs and learning requirements of students.

6.2 Phase-specific arrangements

Device expectations differ between RGS Prep and RGSG.

In RGS Prep, device use is introduced in a phased and age-appropriate way. Expectations should reflect students' age, maturity and level of independence. Adult guidance, classroom structure and parental support remain especially important.

At RGSG, students are expected to bring the required School device to lessons as directed, keep it charged, use it responsibly and maintain it in a condition fit for School use. Expectations for independent organisation are higher, but they remain supported by clear routines and staff oversight, reflecting the age and stage of students across the 11–18 range.

Where the School specifies different device models, accessories or arrangements by year group or phase, those arrangements form part of this policy.

6.3 Digital Levy and School-managed devices

Where the School operates a Digital Levy or equivalent managed-device scheme, that scheme forms part of the School's approach to consistency, safeguarding, support and value.

The School requires students in specified year groups to participate in the managed-device scheme or to use devices that meet the School's stated requirements. This is to ensure compatibility with teaching, safeguarding tools, support arrangements, classroom routines and School systems.

Details of charges, included services, repair arrangements, refresh cycles, insurance, end-of-School arrangements and related practical matters may be set out in supporting documents issued to parents.

6.4 Daily readiness and care of devices

Students are expected to bring the correct device to School when required, fully charged and ready for use.

They are also expected to:

- take reasonable care of the device and any accessories;
- use protective equipment provided or required by the School;
- report faults, damage or loss promptly to the IT Services department through the agreed reporting channel;
- avoid any action that may interfere with the safe or reliable operation of the device; and
- follow School rules and guidance about charging, storage, transport and use.

Parents and carers are expected to support these routines, particularly for younger students.

6.5 Use in lessons and for homework

The School expects devices to be used in ways that support learning, organisation and access. Staff may direct when devices are to be used, when they are not to be used, and how students should move between digital and non-digital activity. Students must follow those instructions promptly.

The School does not assume that every lesson or every task should involve device use. Device use should be purposeful, age-appropriate and educationally justified.

For homework, departments and teachers should work within the School's agreed expectations about where work is set, where materials are stored, and how students are expected to complete and submit work.

6.6 Restrictions, software and technical control

To protect safeguarding, security, reliability and consistency, the School may apply technical restrictions to School-managed devices.

These may include restrictions on software installation, administrator access, the use of unapproved applications, changes to settings, and the use of services that interfere with filtering, monitoring, updates or School systems.

Students must not attempt to bypass, disable or interfere with School technical controls, monitoring arrangements or security settings. Any such attempt will be treated seriously and will lead to disciplinary action and, where appropriate, safeguarding or technical investigation.

6.7 Hotspots, VPNs and alternative connections

On the School site, students must not use personal hotspots, unauthorised connections or services designed to bypass the School's filtering, monitoring or network controls.

The use, installation or attempted use of VPNs or similar services on School-managed student devices is prohibited unless expressly authorised by the School for a specific operational reason. Students who install or attempt to install a VPN will be subject to the School's sanction procedures. These restrictions are in place to protect safeguarding, maintain visibility of risk, preserve system reliability and reduce cyber-security concerns.

6.8 Home use and parental oversight

The School recognises that School-managed devices may also be used at home for homework and other School-related purposes.

Parents and carers remain important partners in setting routines, supervising age-appropriate use and reinforcing expectations.

The School will provide guidance to parents to support them with the management of devices at home. Parents must not make technical changes to School-managed devices or accounts that interfere with safeguarding, management or support arrangements. Parents and carers should report any issues or concerns relating to School-managed devices or their child's device use promptly to the School so that these can be investigated and, where appropriate, supported.

6.9 Device issues, faults and support

The School will set out clear routes for reporting faults, obtaining support and managing repair or replacement issues.

Students and parents must report problems promptly rather than attempting unauthorised fixes or workarounds. Staff should also report recurring technical issues where these affect learning, safeguarding or fairness.

Where a student does not have access to a working device due to fault, damage or other difficulty, the School will manage the issue in line with its support arrangements and available resources.

7. Acceptable use and digital conduct

7.1 General principles

All members of the School community are expected to use digital systems, devices and services safely, lawfully, respectfully and in a way that supports the purposes of the School.

Acceptable use is not limited to technical misuse. It includes honesty, respect for others, responsible communication, protection of privacy, respect for intellectual property, and appropriate use of School systems, devices and digital spaces.

The School recognises that digital conduct may have implications for safeguarding, behaviour, reputation, data protection and assessment integrity. Expectations must therefore be understood as part of the School's wider standards of conduct, not as a separate or optional set of rules.

Use of School systems and devices is a privilege that supports learning and work. The School may restrict access, investigate misuse, apply disciplinary consequences, or require additional safeguards where expectations are not met.

7.2 Staff acceptable use and digital conduct

Staff must use School systems, devices and accounts professionally, securely and in line with their safeguarding, data-protection and conduct responsibilities.

Staff must:

- use only School-approved systems, accounts and communication channels for School business, unless expressly authorised otherwise;
- keep their accounts, devices and credentials secure;
- use School data only for legitimate School purposes and only in appropriate systems;
- maintain professional boundaries in all digital communication with students, families and other stakeholders, including third parties and organisations engaging with the School;
- exercise professional care when using images, video, recorded content or live digital communication, ensuring that all content and interactions are age-appropriate, support student wellbeing and safeguarding, and are consistent with the School's safeguarding policy and KCSIE;
- use digital tools, including emerging and generative tools, in ways that are lawful, professionally justifiable and consistent with School expectations;
- report safeguarding concerns, data breaches, suspected account compromise, technical incidents and misuse through the correct route and without delay; and
- comply with any additional requirements set out in staff-facing specialist policies.

Staff must not:

- share passwords or permit another person to use their account;
- use personal email, personal cloud storage or unapproved services for School-related data, communications, or work;
- use personal channels, personal devices or social-media platforms to communicate with students unless expressly authorised by the School for a legitimate educational or safeguarding purpose; where such communication is authorised, it must be transparent, recorded where appropriate and conducted through School-approved channels;

- introduce new digital services involving School data without the approval of the Director of IT, who will report the change to the IT Strategy Group;
- use School systems to access, create, store or share material that is unlawful, offensive, discriminatory, sexually inappropriate, threatening or otherwise inconsistent with professional standards;
- use digital tools in ways that undermine fair assessment, confidentiality, safeguarding or the reputation of the School; or
- attempt to bypass, disable or interfere with School security, filtering or monitoring arrangements.

All staff are expected to read and acknowledge the Staff Acceptable Use Agreement appended to this policy and to comply with related staff policies governing data handling, account security, monitoring and staff conduct.

7.3 Student acceptable use and digital conduct: RGS Prep

Students at RGS Prep must use School devices, accounts and online services in ways that are safe, kind, sensible and appropriate to their age.

At RGS Prep, acceptable use must be taught, modelled and reinforced through routines, adult guidance and clear explanation. The emphasis is on building good habits as well as setting boundaries.

Prep students are expected to:

- use their School device and account only in the ways they have been taught and directed;
- follow staff instructions promptly when using or putting away devices;
- treat devices carefully and report problems to an adult;
- keep personal information private and tell an adult if they are worried about anything they see, hear or receive online;
- communicate kindly and respectfully;
- use only the sites, apps and services approved or provided for them; and
- behave honestly in all work they complete using digital tools.

Prep students must not:

- try to access inappropriate material or content not intended for them;
- use another person's account or device without permission;
- attempt to change settings, install software, bypass restrictions or interfere with technical controls;
- use digital tools to be unkind, exclude others, upset others or make another person feel unsafe;
- take, share or misuse images, video or messages without permission; or
- use digital tools in ways that misrepresent their own work or conceal what they are doing from staff.

Parents and carers of Prep students play an especially important role in reinforcing routines, supporting home use and reporting concerns. The School will set out age-appropriate student commitments in the Prep student agreement appendix.

7.4 Student acceptable use and digital conduct: RGSG Senior School

Students at RGSG are expected to use School devices, accounts and digital services responsibly, honestly and with good judgement, taking increasing responsibility for their conduct, communication, academic integrity, organisation and care of devices as they progress through the School.

Senior students are expected to:

- bring the required device to School when needed, charged and ready for use;
- use School accounts and digital services only for proper School purposes and in accordance with School rules;
- communicate respectfully with staff and other students;
- use digital tools in a way that supports learning and does not distract from it;
- protect their account details and use only their own account;
- report concerns, harmful material, suspicious activity or misuse promptly; and
- act honestly in all assessed and non-assessed work.

Senior students must not:

- attempt to bypass filtering, monitoring, device restrictions or other technical safeguards;
- use VPNs, hotspots or alternative connections on site where these are prohibited by the School;
- use School systems, accounts or devices to access, store, create or share inappropriate, offensive, abusive, discriminatory or unlawful material;
- use digital communication to bully, harass, intimidate, threaten, exclude or exploit another person;
- take, store or share images, recordings or messages in ways that are intrusive, harmful, disrespectful or unauthorised;
- use another person's account, device or credentials without permission;
- misuse emerging or generative tools in a way that gives a false impression of their own understanding or work; or
- undermine the safe and orderly use of digital systems in lessons, around the School or in relation to School work.

The School will set out senior student commitments in the student agreement appendix. Breaches may be addressed through pastoral, behavioural, safeguarding, technical or assessment processes, depending on the nature of the concern.

7.5 Conduct beyond the School site

The School recognises that digital conduct outside the School site may still affect the safety, wellbeing or reputation of members of the School community, or the orderly running of the School.

The School may therefore respond to off-site digital behaviour where there is a sufficient School connection, including where conduct:

- harms or places at risk a student, member of staff or other member of the School community;
- involves bullying, harassment, abuse, exploitation or intimidation connected to School life;
- affects safeguarding, discipline or pastoral welfare;
- involves misuse of School accounts, data, devices or systems; or
- affects the reputation or legitimate interests of the School.

In responding to such cases, the School will act proportionately and in accordance with its safeguarding, behaviour and disciplinary procedures.

7.6 Sanctions, support and restoration

Where acceptable use expectations are breached, the School may respond in a range of ways depending on the age of the student, the nature and seriousness of the conduct, the context, any safeguarding implications, and whether the behaviour appears deliberate, reckless or repeated.

Responses may include:

- education and re-teaching;
- pastoral support;
- parental involvement;
- restrictions on access to devices;
- restrictions on access to services or digital privileges;
- sanctions in line with the relevant School policy;
- safeguarding action, including referrals to third-party support;
- technical investigation;
- assessment-related action; or
- disciplinary action in the case of staff.

The School will seek, where appropriate, to combine accountability with education, support and restoration. Serious, harmful or repeated misuse, however, will be treated accordingly.

8. Data handling, account security and records

8.1 General expectations

The School handles personal data, confidential information and business-critical information as part of its core work. Everyone who accesses such information through School systems or School processes must do so lawfully, carefully and only for proper purposes.

Staff must understand that data protection is not a technical issue reserved for specialists. It is part of everyday professional responsibility.

School data must be accessed, stored, shared and processed only in ways that are authorised by the School and appropriate to the sensitivity of the information involved.

8.2 Use of School systems for School data

The School's approved digital environment is the default location for School data and School work. School personal data must not be stored in personal email accounts, personal cloud services, unauthorised applications, or unmanaged storage locations. Staff must use School-provided systems and follow the specific rules set out in the School's specialist data and device policies.

The School may permit limited access to School systems from personal devices where this is done through approved methods and in accordance with the relevant staff policy. This does not create a general permission to download, retain or process School data outside School-approved systems.

8.3 Special category and higher-risk data

Some information requires heightened protection because it is particularly sensitive or because the risk of harm from loss, misuse or disclosure is higher.

Staff must take particular care with special category data, safeguarding records, medical information, SEND information, behavioural information, personnel matters, examination information and any other information that is confidential or high risk.

Such information must be accessed, used and shared only where necessary, only by authorised persons, and only through appropriate School systems and procedures.

8.4 Account security

Each user is responsible for the security of any School account assigned to them.

Users must:

- keep passwords and authentication methods secure;
- follow School requirements on passphrases, multi-factor authentication and account use;
- report suspected phishing, suspicious sign-ins, account compromise or unusual activity promptly; and
- take reasonable steps to prevent unauthorised access to screens, devices and accounts.

Users must not share credentials, allow another person to use their account, or attempt to gain access to systems, data or permissions that have not been authorised for them.

8.5 Monitoring, logging and investigation

The School may monitor, log and review the use of its systems, devices, accounts and digital services for safeguarding, security, operational, investigative and legal reasons.

Monitoring is carried out to protect students, staff, the School's systems, and the integrity of School operations. It may also be used to investigate suspected misuse, incidents, policy breaches or technical problems.

Any access to monitoring information must be lawful, proportionate, role-appropriate and limited to legitimate purposes.

8.6 Data breaches and incidents

Any actual or suspected loss, unauthorised disclosure, alteration, compromise or unavailability of School personal data must be reported immediately through the School's data-breach route, via the DPO mailbox (dpo@rgsg.co.uk).

Staff must not delay reporting while they investigate the issue themselves or decide whether it is serious enough to report. Prompt reporting is essential so that the School can assess risk, protect individuals and meet any legal obligations.

Loss or compromise of a device containing School data, or exposure of School data through an unapproved digital service, must be treated seriously and reported immediately.

8.7 Records, retention and continuity

The School will retain and delete records in accordance with its Information and Records Retention Policy and any applicable legal or regulatory requirements.

Staff must store work and information in locations that support continuity, handover and appropriate retention.

School systems should be used in ways that support resilience, continuity and good records management rather than personal convenience.

8.8 Leavers, transfers and access changes

When a member of staff or student leaves the School, changes role, is absent for a substantial period, or no longer requires access to a system, the School will manage accounts, permissions, data access and device arrangements in line with its operational and security procedures.

Accounts that are inactive (where a user has not logged in or used any School services) for 90 days, not including holidays or other agreed periods of leave, will have their account automatically deactivated. Staff who have left the School will have their account access disabled and all data deleted from their mailbox and OneDrive within 90 days.

Managers and relevant staff must ensure that business continuity, handover and data transfer are considered in good time. Access should not be retained longer than necessary.

8.9 Further detail

Detailed operational rules on data handling, approved services, personal devices, account lifecycle, password practice, removable media, incident reporting and records management are set out in the School's specialist policies and procedures, including the Staff Data Handling and Device Use Policy. Those documents form part of the School's overall digital and data control framework and must be followed.

9. Emerging tools and services

9.1 Approach

The School recognises that new digital tools and services, including generative technologies, may offer educational and operational benefits. The School also recognises that such tools may create safeguarding, privacy, reliability, quality, workload or assessment risks if introduced without proper review.

No new service that involves School data, student use, staff use in School business, or integration with School systems should be adopted informally or by personal preference alone.

The School will therefore maintain a defined process for the review, approval and oversight of new digital services.

9.2 Approval before use and adoption

Any proposed new digital tool, application, platform or service must be reviewed before it is used for School purposes where it involves:

- School personal data;
- student access or student-generated content;
- staff use in teaching, learning, communication, administration or assessment;
- integration with School systems or accounts; or
- any meaningful safeguarding, operational or reputational risk.

Staff must not upload School data to, or require students to use, a new service before that review has taken place and approval has been given by the Data Protection Officer and the Director of IT; the DPO will report new approvals to the IT Strategy Group.

9.3 Review criteria

In deciding whether a service is suitable for School use, the School may consider:

- safeguarding implications;
- age appropriateness;
- privacy and data-protection compliance;
- security and identity management;
- educational value;
- accessibility and inclusion;
- reliability and technical support;
- impact on workload and consistency;
- compatibility with existing systems;
- contractual and procurement considerations; and
- implications for assessment integrity.

Approval may be limited by phase, age group, purpose, category of data, or named staff roles.

9.4 Generative and adaptive tools

The School recognises that generative and adaptive digital tools require particular care.

Such tools may assist with planning, explanation, accessibility, feedback, administration or student support. They may also generate inaccurate, misleading, inappropriate or biased content, and some services may create serious data-protection or safeguarding concerns if used inappropriately.

The School will therefore distinguish between:

- tools approved for use with School personal data;
- tools approved for specified educational use without personal data;
- tools that may be explored by staff on a personal account without School data;
- tools approved for limited student use; and
- tools that are not approved for School use.

Staff and students must follow the rules that apply to the category into which a tool falls. The School may change those categories over time.

9.5 No assumption of entitlement

No member of staff or student is entitled to use a digital tool for School purposes simply because it is popular, technically available, personally preferred or free to access.

The School may refuse, limit, suspend or withdraw approval where this is justified by safeguarding, educational, legal, technical or operational concerns.

9.6 Review and withdrawal

Approved services should be kept under review. The School may revisit an approval decision if circumstances change, including where there is:

- a safeguarding concern;
- a data-protection concern;
- a significant change to service terms or ownership;
- evidence of poor reliability or poor educational value;
- misalignment with School systems or policy; or
- repeated misuse.

Where appropriate, the School may withdraw approval, require migration to another system, or impose additional conditions of use.

10. Assurance, monitoring and review

10.1 Governance and assurance

The School will maintain oversight of digital and data practice through appropriate leadership review and governor assurance.

This should include attention to:

- online safety and safeguarding trends;
- filtering and monitoring arrangements;
- data-protection incidents and themes;
- cyber-security issues and account security;
- device provision and operational effectiveness;
- assessment-related issues involving digital tools;
- staff training and implementation;
- feedback from staff, students and parents; and
- progress against agreed digital priorities.

The purpose of assurance is not only to check compliance, but to identify patterns, weaknesses, unintended consequences and areas for improvement.

10.2 Monitoring implementation

Senior leaders and relevant policy owners should monitor whether this policy is understood and implemented in practice.

This may include:

- review of incidents and casework;
- audit or sampling of practice;
- review of technical controls and their use;
- learning walks or quality assurance activity where relevant;
- staff and student feedback;
- parental feedback; and
- periodic review of alignment between policy, systems and actual practice.

Where inconsistency or ambiguity is identified, the School should respond by clarifying expectations, improving systems, refining guidance or strengthening training.

10.3 Policy review

This policy will be reviewed at least annually and may be reviewed earlier where necessary.

An earlier review may be required where there is:

- a significant change in statutory guidance, regulatory expectations or current standards;
- a material safeguarding, cyber-security, data-protection or assessment incident;
- a significant change to the School's digital systems or device arrangements; or
- evidence that the policy is no longer sufficiently clear, workable or effective.

The School may also update annexes, appendices or supporting guidance between full policy reviews where this helps keep practice current and coherent.

11. Communication and training

11.1 Communication

The School will communicate this policy, and the expectations arising from it, in ways that are appropriate to different audiences.

This includes communication with:

- staff, through induction, training, internal guidance and routine leadership communication;
- students, through age-appropriate explanation, teaching, assemblies, tutor time, classroom routines and signable agreements; and
- parents and carers, through policy publication, supporting guidance and practical communication where needed.

11.2 Staff training and induction

Staff must receive appropriate induction and ongoing training in relation to digital safeguarding, acceptable use, data handling, account security, assessment integrity and the safe use of emerging digital tools.

Training should be proportionate to role and responsibility. Some staff will require additional or more specialist input because of their leadership, safeguarding, technical, data or assessment functions.

Where systems, risks or expectations change, the School should provide timely communication and, where necessary, updated training.

11.3 Student education

Students must be taught how to use digital systems and services safely, responsibly and effectively. This should include online safety, digital conduct, privacy, reporting concerns, organisation, academic honesty and the appropriate use of digital tools in learning and assessment.

Teaching should be age-appropriate, reinforced over time and aligned with the actual systems and expectations students experience in School.

12. Digital operations, support and printing

The School operates a central IT Help Desk as the first point of contact for routine IT and audio-visual support. Staff, students, visitors and contractors must use the School's designated support route for such requests and must not rely on informal arrangements.

School-hosted online events requiring technical support must use School-approved platforms and arrangements. External presenters and other third parties using School systems or equipment must comply with the School's relevant acceptable use and data-handling requirements.

The School operates a managed printing and photocopying environment. Printers, photocopiers and associated services used for School business must be procured, configured and supported through the School's approved arrangements; privately sourced or unmanaged devices must not be connected to the School network or used for School data.

Staff and students are expected to minimise unnecessary printing and to use secure digital distribution where this is reasonable and appropriate. Where printing is necessary, it must be carried out in a way that protects confidentiality, supports secure release, and complies with the School's data-handling, records and assessment requirements.

Operational detail, including support arrangements, event setup, printing processes and consumables, will be set out in separate internal guidance maintained by IT Services.