Digital Safety Policy

September 2024

1 Purpose

RGSGD aims to enable all pupils to use digital technology effectively, appropriately and safely to enhance their learning and to prepare them for a future of continuing digital innovation.

- RGSGD will provide a safe and secure environment for pupils to learn and explore digital technology.
- We will educate all pupils, staff and parents on the appropriate use of digital technology within the school community and provide clear protocols on appropriate and acceptable use.
- We will help protect pupils, staff and parents by seeking to raise awareness of the key risks and emerging issues and the actions that can or should be taken to protect young people and mitigate those risks.

2 Scope

This Digital Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school-based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard pupils, staff and parents.

It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable or misuse of these technologies by pupils, staff or parents.

3 Risks

There are always going to be risks with using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils use these technologies. These risks include but are not limited to

- Being vulnerable to inappropriate contact from strangers and online grooming;
- Sharing personal details and information with strangers;
- Cyber-bullying;
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices;
- Issues with spam and other inappropriate email;
- Online content which is abusive, offensive, or pornographic;
- Sexting
- Online gambling;
- Uncontrolled expenditure e.g. through in-game purchases;
- Attempting to circumvent age restrictions on social media and other platforms;
- The use of social media to encourage extremism; and
- Viruses, malware, ransomware and phishing.

It is also important that staff are clear about appropriate use of digital technology when communicating with pupils, for example only contacting pupils about homework via a school email address or the School's other online systems and remote learning technologies and never to use personal email addresses.

Whilst RGSGD endeavours to safeguard and mitigate against all risks, we will never be able to completely eliminate them. Any incidents that may come to our notice will be dealt with quickly and according to the school’s policies.

4 Pupils

Our pupils are:

- involved in the review of our Digital Safety Agreement in an age appropriate way;
- responsible for following the Digital Safety Agreement and required to sign that they have read and understood the rules;
- taught to use the internet in a safe and responsible manner.
- taught to immediately tell an adult about any inappropriate materials or contact from strangers
- made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;
- taught and encouraged to consider the implications for misusing the internet eg posting inappropriate materials;
- taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for schoolwork, and be copyright free;
- taught to understand what is meant by e-safety through age appropriate delivery;
- taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police;
- taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk;
- given explicit guidelines and procedures for using mobile phones and other personal devices in School and are expected to abide by our Digital Safety Policy; and

5 Inappropriate use by pupils

Should a pupil be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a pupil accidentally accessed inappropriate materials, the pupil is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window.

Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour Policy

Refer to Annex 1 for further guidance.

6 Staff

It is the responsibility of all adults within the school to:

- Adhere to the Staff Code of Conduct including Acceptable Use;
- Implement the pupil Digital Safety Agreement (see Annex 2, 3 and 4);
- Be up to date with digital knowledge appropriate for different age groups;
- Be vigilant when using technology as part of lessons;
- Model safe and responsible use of technology;
- Provide reminders and guidance to pupils on Digital Safety;
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner;
- Not leave a computer or other device unattended whilst they are logged on;
- Lock away or safely secure all portable ICT equipment when not in use;
- Not connect with any RGSGD pupil on social networking site, or via personal mobile phones and follow the School's Social Media Guidelines. See Annexe 5 for further detail;
- Protect confidentiality and not disclose information from the network, or pass on security passwords;
- Make sure that any information subject to Data Protection is not stored on unencrypted portable media or transported in an insecure form;
- Use their discretion when communicating electronically about work-related issues and not bring the School's reputation into disrepute;
- Follow the School's 'dos' and 'don'ts' in our Email Best Practice Guide – see Annex 6;
- Not make or take personal calls or engage in personal texting when they are on duty;
- Report any concerns about a pupil related to safeguarding and e-safety to the Designated Safeguarding Lead;
- Report accidental access to inappropriate materials to the IT team so that inappropriate sites are added to the restricted list; and
- Only use school owned devices and memory cards to take photographs, videos or audio recordings, and only where parents have given permission for photos/videos to be taken.

7 Inappropriate use by staff

- If a member of staff is believed to have misused the internet or network in an abusive or illegal manner using School systems or equipment, a report must be made to the Principal immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.
- Refer to Annex 1 for further guidance.

8 Parents and visitors

- All parents have access to a copy of this Digital Safety Policy on our website. Parents are asked to explain and discuss their child's learning and understanding of how to use online technologies safely and the school rules with their child, so that they are clearly understood and accepted.
- As part of the approach to developing e-safety awareness with pupils, the School may offer parents the opportunity to find out more about how they can support the School to keep their child safe whilst using online technologies beyond school;
- Parents should be aware that the School cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the School so we can offer advice and support. The School has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

9 IT Department

The staff in the IT Department have a vital role to play in implementing the technical aspects of the Digital Safety Policy. In particular the IT team will ensure that:

- The servers, databases and network are secure and protected from malicious attack.
- User accounts are only opened with appropriate authorisation, are granted the appropriate level of access and permissions for the role and are closed promptly when no longer required.
- Only sufficiently strong passwords are used and that they are regularly changed, and that additional access controls are used as appropriate.
- The School meets all technical requirements required by UAE Online Safety Guidance and Cognita Guidance.
- That software is kept updated to ensure the latest security patches are implemented to address any new vulnerabilities.
- That the internet filtering and fire wall is active at all times, is set at the appropriate levels and is kept up to date.
- They maintain an awareness of new and emerging online safety issues, potential vulnerabilities and the technical solutions that may need to be deployed. They will ensure that, as appropriate, other staff are made aware of new and emerging issues and mitigating measures.
- That the safety and security of the Schools' digital environment is routinely tested and checked to ensure that the deployment of the security features is effective.

10 Wi-Fi access for visitors

- Parents and visitors to the school are expected to abide by this policy. Should visitors wish to access the internet via the School's Wi-Fi, they will be issued with a password. Access is only permitted once they have agreed to the school's terms and conditions.

11 Video and photography at school events

- Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission.
- Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

12 Early Years Use of Mobile Phones or Device - Statutory regulation

- The Early Years Safeguarding and Welfare Requirements (para 3.4) requires all schools to have a clear policy on the use of mobile phones and devices.
- The Cognita Code of Conduct for staff states, 'Cognita does not permit the use of personal mobile phones and cameras by staff where children are present'.

13 Filtering and safeguarding measures

- The School's internet has a robust filtering system which is set at an age appropriate level such that inappropriate content is filtered.
- The system logs all attempts to access the internet, including all attempts to access inappropriate content.
- Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a regular basis.
- Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users.
- Strong encryption is used on the wireless network to provide good security.

14 Email use

- The school provides school email addresses for pupils from Year 3 to promote safe and efficient communication in the school.
- All staff are expected to use email professionally and responsibly. See Annexe 6 for further details.

15 The School's use of images and videos

The school abides by the UK Data Protection Act 1998 and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw their permission at any time by informing the administration team in writing at a specific campus.

Staff are not permitted to use their own devices or memory cards to record videos or photographs of pupils, and when storing images within the School's network are requested to only use the pupil's first name.

16 The curriculum and tools for learning

The school teaches our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSPEE lessons. The following concepts while explicitly taught in ICT, may be covered in other subjects. These skills and competencies are taught through the school in an age appropriate manner, they may include:

- Digital citizenship;
- Future work skills;
- Internet literacy;
- Making good judgments about websites and emails received;
- Knowledge of risks such as viruses, and opening mail from a stranger;
- Access to resources that outline how to be safe and responsible when using any online technologies;
- Knowledge of copyright and plagiarism issues;
- File-sharing and downloading illegal content;
- Uploading information – knowing what is safe to upload; and
- Where to go for advice and how to report abuse.

Further details about the content of the curriculum related to ICT can be found in the ICT and PHCE curriculum documentation.

17 Monitoring

It is the responsibility of the school to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. The school will monitor the use of online technologies and the use of the internet by pupils and staff.

The Designated Safeguarding Lead, ICT teachers and lead pastoral staff will conduct regular audits with pupils to assess their knowledge and understanding of issues related to e-safety and act on any areas of vulnerability.

To audit digital safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of e-safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all pupils demonstrate an awareness of e-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?

- Is the current wording fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is e-safety observed in teaching and present in curriculum planning documents?

Annexe 1 – Digital Safety Agreement for Pupils in EYFS and Year 1

EYFS and Year 1: Digital Safety Agreement

These are our rules for using the internet safely at school:

- We use the internet safely to help us learn.
- We learn how to use the internet.
- If we see anything on the internet, or receive a message, that is unpleasant, we must tell an adult.
- We learn to keep our password a secret.
- We know who and when to ask for help.
- If we see something on a computer that we do not like or makes us feel uncomfortable we know what to do.
- We know that it is important to follow the rules.
- We aim to look after each other by using the internet safely.

Annexe 2 – Digital Safety Agreement for Pupils in Years 2 to 12

Year 2 - 12: Digital Safety Agreement

I am encouraged to use and be aware of the safety rules and procedures which regulate my use of the ICT resources, including the internet. Access to the school's network and the internet enables me to find resources, to communicate, and to help my research for the completion of school work.

I accept that these facilities are to be used for educational purposes only and in an appropriate manner. I take responsibility for my actions and know that any breach of the rules will be considered a serious disciplinary matter.

- I accept that the school monitors my use of the internet at school and my school email account.
- I am responsible for the websites that I use and I only access those appropriate for my age.
- I will not use a personal device or mobile phone whilst on school property.
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to anyone.
- I will follow fully our teachers' instructions over the use of IT and the internet.
- I will not assume that information published on the Web or written in an email is accurate, including people's details.
- I keep my username and password confidential.
- I am careful about what I write on a computer. I check my work before I print or send it.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I do not make available online personal information about myself or anyone else, such as an address, telephone number and private details, in an email or on a website.
- I will only engage in age appropriate use and will always represent myself with integrity
- I do not respond to offensive, abusive or rude messages. I let a teacher know immediately if I am sent anything I do not feel comfortable with.
- I do not access sites/download materials which are in bad taste, offensive, violent or pornographic.
- If I quote from a text I will always attribute my sources, cite the author, using quotation marks, and compiling a bibliography as required.
- I will never plagiarise another person's work.
- I always respect the privacy of other users' data.
- I will report to a teacher any incident that breaches the Digital Safety Agreement, even if that incident does not affect me. If I accidentally access inappropriate content, I will minimise the window and alert a teacher immediately.
- I will treat school IT equipment with respect and will report any damages to a teacher. (deliberate damage will be charged)
- I will not bring the school's name into disrepute.
- I will not install any applications/programs/VPNs that contravenes the School's network.
- I will check my school emails regularly to enable me to work and learn effectively.
- I know that if I am worried about something related to technology outside of school I can ask for advice or help from my teachers.
- I understand that it is against the law to post malicious/insulting/indecent messages on social media and that I may be held legally responsible for those comments and any replies.

Name: _____ Year group: _____

Parent signature: _____

I understand the contents of the school's Digital Safety Agreement and the rules for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature: _____ Date: _____

Annexe 3 - Social Media Guidance

Social media is a broad term for any online platform which enables people to directly interact with each other.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and pupils.

Scope

This guidance is subject to Cognita's Staff Code of Conduct including Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly represent the school;
- Applies to such online communications posted at any time and from anywhere;
- Encourages the safe and responsible use of social media through training and education; and
- Defines the monitoring of public social media activity pertaining to the school.

RGSGD respects privacy and understands that staff and pupils/pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this guidance. Personal communications which do not refer to/ impact upon the school are outside the scope of this guidance.

Digital communications with staff/pupils are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes, but must consider whether this is appropriate and consider the potential implications.

Process for creating new accounts and monitoring use

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "friends of the school" Facebook page. Anyone wishing to create such an account must present a case to the Principal which covers the following points:

- The aim of the account;
- The intended audience;
- How the account will be promoted;
- Who will run the account; and
- Will the account be open or private/closed.

Following consideration, an application will be approved or rejected. In all cases, the Principal must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

School accounts must be monitored regularly and frequently to ensure appropriate use.

Annexe 4 – Social Media Do's and Don'ts

Managing your personal use of social media

- 'Nothing' on social media is ever truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online, consider: scale, audience and permanency.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

The Do's:

- Check with a senior leader before publishing content that may have controversial implications for the school;
- Use a disclaimer when expressing personal views;
- Make it clear who is posting content;
- Use an appropriate and professional tone;
- Be respectful to all parties;
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author;
- Express opinions but do so in a balanced and measured manner;
- Think before responding to comments and, when in doubt, get a second opinion;
- Seek advice and report any mistakes using the school's reporting process; and
- Consider turning off tagging people in images where possible.
- Ensure all social media content is tolerant of all beliefs and cultures, especially those if the UAE

The Don'ts:

- Don't make comments, post content or link to materials that will bring the school into disrepute;
- Don't publish confidential or commercially sensitive material;
- Don't breach copyright, data protection or other relevant legislation;
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content;
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content; and
- Don't use social media to air internal grievances.
- Do not publish photos of others without permission

Annexe 5 – Email etiquette

Email best practice

The Do's:

- Communicate in person where possible – face to face or video conferencing, or phone
- Write well-structured emails and use short, descriptive subjects.
- Sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. The use of internet abbreviations and characters such as smileys is not encouraged.
- Signatures must include your name, job title and school name. A disclaimer should be added underneath your signature.
- Ask for advice from a colleague if you are unsure re the content (given the email is not confidential)
- Users must spell check all mails prior to transmission.
- Only mark emails as important if they really are important.
- Avoid long strings of messages; start new conversations.

The Don'ts:

- Write an email if you are feeling angry/upset.
- Write it in an email unless you would put it on a noticeboard in the office or in a newspaper.
- Write anything that is libellous, defamatory, offensive, racist or obscene - you and the school can be held liable.
- Forward confidential information - you and the school can be held liable.
- Forward a message with sensitive information without acquiring permission from the sender first.
- Use reply all unless approved by SLT.
- Send email messages using another person's email account.

Annexe 7: Procedures for staff in the event of a breach of this policy by a pupil or adult

(A) An inappropriate website is accessed inadvertently:

- Report to DSL; and
- Contact ICT Support via email so that it can be added to the banned or restricted list.

(B) An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material, by shutting down the computer;
- Record the incident in writing;
- Report to the Principal and DSL immediately; and
- The Principal applies the Behaviour Policy.

(C) An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity;
- Alert the DSL immediately; and
- Ensure the device is shut down and record the nature of the material.

(D) An adult has used ICT equipment inappropriately:

- Follow the procedures for (B).

(E) An adult has communicated with a pupil, or used ICT equipment, inappropriately:

- Ensure the pupil is reassured;
- Report to the Principal who should follow the Staff Code of Conduct and Safeguarding Policy (if relevant);
- Preserve the information received by the pupil if possible, and determine whether the information received is abusive, threatening or innocent; and
- If illegal or inappropriate use is established, contact the Principal or the Cognita Director of Education, if the allegation is made against the Principal, and the Designated Safeguarding Lead immediately, and follow the Safeguarding Policy.

(F) Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school:

- Preserve any evidence; and
- Inform the Principal immediately and follow the Safeguarding Policy as necessary.

(G) Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere:

- The Principal should be informed.

Author	
Document author	Cognita
Date of publication	September 2024
Review date	September 2026

Audience	
Audience	Staff, Parents, Pupils

Consultation (if appropriate)	
Consultees	

Related documentation	
Related RGSGD documentation	
Related external documentation	

Connections	
Connection with inspection framework	
Connection with national agenda	n/a