Digital Device Responsible Use Agreement (DDRUA) Policy

Vision: Grow - Flourish - Succeed
Mission: Together we inspire creative, mindful learners who value diversity, support one another and strive for success.

1. Introduction

GEMS Founders School, Dubai (GFS), recognises that access to technology in school gives students greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship. We are committed to creating a 21st century learning environment to provide equitable access to technology that will aid our students in becoming self-directed learners, collaborative team players, and information producers, as well as information consumers. The application of digital technologies to teaching and learning at GFS is designed to enrich student learning through internally housed resources and the effective utilisation of wider online resources.

Definition of Digital Devices

The definition of Digital Devices includes but is not limited to, the following: desktop computers, handheld devices such as iPads, laptops, mobile phones, MP3 players and all other devices which have the capacity to access the Internet or store digital data in any format. We at GFS recognise that due to the rapidly changing nature of technology, new forms of devices may become available in the future. GFS reserves the right to include all such devices within the scope of this policy, as and when necessary.

2. Purpose of policy

The purpose of the GFS Digital Device Responsible Use Agreement is to ensure all students use technology in GFS effectively, safely, legally and responsibly, to facilitate learning and to help ensure that they develop the attributes of competent digital citizens. The DDRUA provides guidelines for using digital hardware and software on individual computers/devices, on local area networks, wide area networks, wireless networks, the Internet and companion technological equipment (e.g. printers, servers, whiteboards, projectors, etc.) when students are at GFS. The agreement also establishes rights and responsibilities for all users. All users of the GFS network and technological devices anytime, anywhere, are expected to follow the guidelines or risk loss of digital privileges. In cases of serious breaches, further action may be taken, in line with the GFS standard disciplinary procedures.

The signatures on the DDRUA summary are binding and indicate that the parties who signed have read the terms and conditions and understand their meaning.

Users who knowingly access prohibited information or who disregard guidelines will be subject to disciplinary action.

3. Aims and objectives

At GFS, we aim to educate our pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe when using digital devices, in and beyond the context of the classroom.

For students to use the GFS technology resources, they must follow the guidelines set forth in this DDRUA. The rules written in this agreement are not all-inclusive. GFS reserves the right to change this agreement as and when it deems it necessary to do so. It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical and legal manner. By using any digital resources, whether owned personally or by GFS, users acknowledge their understanding of the DDRUA as a condition of using such devices and the Internet.

At GFS we will:

- Provide a systematically filtered service for students.
- Provide supervision and direction in activities which use the Internet.
- Have an Information Literacy program focused on effective use of internet sources/sites.
- Adopt programs that promote safe and ethical behaviours about digital rights and privacy information.
- Set tasks that require students to problem solve through challenging and open questions requiring more than copied and pasted responses from the Internet.
- Reinforce the importance of safe, disciplined, ethical, responsible and respectful use of the Internet in all curriculum areas.
- Provide support to parents to understand this agreement (e.g. language support).
- May allow student access to social networking sites for educational purposes – this will be under teacher direction with clear protocols established

The guidelines provided in this DDRUA are intended to help users understand appropriate use. GFS may restrict, suspend, or terminate any user's access to GFS's computer systems upon violation of the DDRUA. This policy applies to all digital resources, not only the computers, devices and equipment provided in the GFS's hardware provision, but also the personal devices students bring to GFS in accordance with GFS's bring your own device (BYOD) initiative.

4. Responsibilities

User:

- Show respect and courtesy for other users in GFS's community, which includes the strict prohibition of cyber bullying and harassment.
- Recognize and respect the property of others.
- Comply with legal restrictions regarding the use of social media in the UAE. See the TRA guidelines UAE Digital Content Laws. Comply with legal restrictions regarding plagiarism, intellectual property and the use and citation of information resources and copyright law.
- Use non-curriculum relevant materials only outside of GFS and without detriment to their studies - GFS recognizes the benefits of students being permitted to personalise the content on their own devices, however, this is subject to a strict adherence to the expectation that the primary purpose of such devices is to facilitate learning.
- Help maintain the integrity of the GFS network and equipment.
- Avoid tampering or experimenting with the GFS network or equipment, including efforts to bypass GFS's Internet filters or proxies.
- Make personal devices available for inspection by an administrator or other staff member upon request.
- Use appropriate language in all communications.
- Never use or attempt to use another student's assigned hardware, subscriptions, logins, files, or personal information.

- Never give out personal information, such as name, address, photo, or other identifying information online, including username and password.
- Never use their personal devices or equipment to record (audio/visual) others without their permission.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- No device will be used to record any member of the GFS community without prior permission. If any user should record any person with permission, appropriate dispensary action will be taken.
- **Non-adherence to the provisions of this DDRUA will result in disciplinary action in accordance with GFS's standard procedures.**

Accounts:

Users are expected to comply with the following rules regarding their GFS network accounts.

- School related files are the only files to be saved in a student's personal folder.
- Users should not store commercial software, music, and/or games or hidden files to their folders.
- Accessing and playing commercial/online games is not permitted.

Respect for Others:

Users should respect the rights of others using the technology resources.

- Always log off your workstation.
- Never deliberately attempt to disrupt network performance or interfere with the work of another user.
- No device will be used to record any member of the GFS community without prior permission. If any user should record any person with permission, appropriate dispensary action will be taken.

Respect for Property:

Students are responsible for their own devices while in school:

- Devices should be transported throughout GFS safely.
- A student is to be accountable for any damage that occurs to their device while in GFS. It is the responsibility of all users to safeguard their personal and GFS owned equipment from loss, theft or damage.
- Accessing or using other students' devices is prohibited.
- Ensuring their device has sufficient charge for use in lessons and is only used in supervised lessons.

Software Installation:

Software may only be installed on the school information systems (including all individual workstations) with prior approval from the IT (Information Technology) Department.

Software Copyright:

- The only software, other than students' projects, to be used on the school computers are those for which the school owns a valid license or has approved from an open-source solution.

- Licensed/copyrighted software is not available for borrowing and may only be used at other sites with approval of the IT Technician.
- Copyrighted software shall not be downloaded from the Internet or further transmitted in any form without compliance with all terms of a preauthorised licensing agreement. Infringement or violation of UAE or international copyright laws or restrictions will not be tolerated.
- Any attempts to circumvent the licensing control or the copying of software from the network without the IT Department's permission is prohibited.
- Installation of software and applications on students' own devices is permitted insofar as it does not conflict with the security requirements outlined above or the primary purpose of such devices as learning tools.

Hardware:

- Report equipment problems immediately to a teacher or the Computing Department.
- Leave workstations and peripherals in their designated places.
- Keep work areas neat and clean and free from food and drink.
- Any attempts to move, repair, reconfigure, modify or attach external devices to existing information and network systems without the Network administration and/or Computing Department's permission is prohibited.
- Borrowing of school hardware is not permitted unless authorization has been given from the IT department.

Artificial Intelligence (AI):

The purpose of this AI section is to outline our AI code of ethics, provide guidelines for the ethical and responsible use of AI tools within GEMS Founders school. This ensures that students, teachers and staff use AI to enhance learning, teaching and administrative processes while maintaining high standards of integrity and security.

- AI use must comply with **GEMS Examination Board Integrity Standards** (AQA, Edexcel, OxfordAQA, IB, etc.).
- Students must disclose AI assistance when required by teachers or exam boards.
- AI-generated work must not be submitted as original work unless explicitly permitted.
- AI misuse is now categorized under **Academic Honesty Violations.**

AI Code of Ethics:

At GFS...

- AI tools, including ChatGPT, should be used in a way that aligns with the principles of digital citizenship. This includes being responsible, respectful and ethical.
- We recognise that AI may reflect biases or inaccuracies in its responses based on its training data. We are mindful of this and critically evaluate the information provided by AI tools.
- We use appropriate language and treat others with respect. We do not use AI to harass, bully, or discriminate against others. We verify information before sharing it with others. We do not use AI to spread false information or engage in deception.
- We clearly define the problem or question we are trying to solve to help create more specific and effective questions.
- We remember that AI is a tool with limitations. We use AI to help us learn and explore new ideas but do not rely on it as the sole source of information.

- We engage in active learning by asking follow-up questions and seeking to deepen our understanding of the topic.
- We are mindful of the information we share with AI and we protect our/other's privacy by not sharing personal or sensitive information.
- Our related policies will be in alignment with those of Examination/Curriculum Boards ensuring use of AI tools complies with the guidelines set by various curriculum boards but not limited to AQA, Pearson Edexcel, OxfordAQA.

Misuse of AI:

- We do not use AI tools to complete assignments or projects meant to be completed independently unless explicitly instructed to do so by a teacher.
- We understand that the misuse of AI includes, but is not limited to, using AI to cheat on exams, plagiarise work, generate inappropriate content or manipulate test scores.
- We understand that any form of AI misuse, such as generating and disseminating false information or engaging in cyberbullying, will result in disciplinary action.
- Students are prohibited from using AI to impersonate others or create false identities.

Consequences of misuse:

- Violations of the AI policy will result in disciplinary actions aligned with GFS's standard procedures. This may include loss of technology privileges, suspension or other appropriate actions.

Educational Integration:

- We will educate stakeholders on the ethical use of AI tools in accordance with these guidelines.
- We will ensure Staff and educators have received training and professional development opportunities to understand AI systems and their applications.
- We will encourage teachers to incorporate AI technologies into their teaching practices when appropriate.

As the integration of AI into educational practices advances, GEMS Founders School, Dubai remains committed to its responsible and effective use. This policy promotes an environment where AI tools are used to enhance the learning experience, improve operational efficiency and foster an inclusive, safe and engaging educational atmosphere. Adherence to this policy by all stakeholders is imperative for maintaining the quality of education and the integrity of GEMS Founders School, Dubai. Together, we can connect the power of AI to create a better future for our students while preserving the values that make us good human.

5. Mobile phones

The school has a zero-tolerance approach to mobile phone usage by students in school; mobile devices are therefore allowed in school for emergency purposes only.

Primary

Mobile phones are not permitted for primary students. If a primary student should need to communicate with their parent / guardian, this will be done under the supervision of school staff.
If a primary student is found with a mobile phone, it will be confiscated, and parents will be asked to come to the school to collect from the relevant staff member.

Secondary

Should a secondary school-aged student be required by parents to carry a mobile phone to be able to contact parents outside of school hours, the mobile phone should be kept securely in a bag and turned off for the duration of school hours. If seen in use, mobile phones will be confiscated from students and returned to parents. In the event of an emergency, students may use their phones to contact their parents with permission from a staff member.

Mobile phones are not considered appropriate devices to support student learning at the school- please see section 8 (Use of BYOD) of this policy regarding what are considered appropriate devices.

GFS emphasizes that it accepts no responsibility for any loss or damage to phones while they are on school premises.

- During lessons, form times and breaks mobile phones must be switched off to prevent them from becoming a distraction.
- Parents and other contacts must not attempt to contact students via their personal mobile unless in absolute emergencies.
- Parents needing to pass on an urgent message during school hours should contact GFS reception.
- The school allows staff to bring in personal mobile phones and devices which may only be used during non-contact time or for emergency purposes.
- Under no circumstances does the school allow a member of staff to contact students or parents using their personal email or number.
- Users bringing personal devices into school are responsible for ensuring that there is no inappropriate or illegal content.

6. Internet/World Wide Web usage

The Internet is a global network of digital devices linking users to schools, businesses, universities and other sites. GFS recognizes many sites have educational uses, while others do not. GFS wishes to respond to this by encouraging use of sites for educational reasons only. Required standards of conduct include:

a. The school acknowledges that access to the Internet is a privilege and not a right.
b. Use of devices is limited to lesson time. Devices are not to be used in corridors, common areas, on buses or whenever a member of staff has not directly instructed the use.
c. Respect the use of copyrighted materials.
d. Respect the rights and privacy of others.
e. E-mail and social networking are allowed during GFS hours only in connection with a classroom assignment.
f. Downloading of unauthorised programs, software or digital content is not allowed to be held on devices registered for use in GFS.
g. Compromising the security of GFS in any manner is unacceptable.
h. Respect the values and ethics of the local culture.
i. You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended use or audience.
j. Names or personal details of colleagues, parents or children will not be acquired through any online medium on school site. If students are required sign up to educational sites, they will use their own school email, as appropriate.
k. Online gaming, other than for educational purposes will not be permitted on school site.
l. No Social Media pages with any connection to GFS should be set up by any staff, student or parent.

A violation of the above standards and any others included in the DDRUA will result in a denial of access and possible further disciplinary action.

If students fail to meet these standards, they will have to take relevant courses to access their devices again in school.

- First offence – the student will have to undertake relevant courses set by the school. This course will have to be signed by both student and guardian to show completion of the course.
- Second offence – students will be prohibited from using their devices in school for a specified period.

7. Personal equipment

All users must follow all policies even while using their own personal equipment.

- Watching DVDs, Movies, TV Shows, playing online games etc. while at GFS is prohibited unless directed by GFS staff
- Private networks are prohibited within the school network unless users get permission from the IT department.

8. Use of BYOD

Students in all grades (FS to 13) can take advantage of GFS's bring your own device (BYOD) initiative.
All students and parents will be required to sign the GFS Digital Devices Responsible Uses Agreement Summary prior to activation of the students' access privilege.

- BYOD at GFS is currently limited strictly to one device per student. Mobile phones may be used if the device is out of charge or not working if teachers allow.
- Students should bring in their device with either Android, Windows or iOS operating systems.
- We would advise that students in KS3-5 to register a laptop due to its increased functionality for creation.
- Parental guidance and recommendations regarding the suitability of devices can be provided on request from the ICT and computing department.
- Students will be held responsible for maintaining their own devices and keeping them in good working order whilst in their possession.
- The school will be responsible for repairing only school owned mobile devices which malfunction. Mobile devices which have been damaged from student/staff misuse or neglect will be repaired with cost being borne by the student/staff. In the event of an accidental damage, the school on a case-to-case basis may exercise discretion in recovering the cost of repair to the device from the user.

At GFS we require all children to have their own device to access their learning at home and in school. The school endeavours to support students, where possible. All devices will be properly sanitised each day before given to a student.

9. Charging devices

Students should come to GFS with their devices fully charged to minimise time lost due to devices needing to be recharged. However, in the event of a students' device running out of charge, students can bring in their own power banks. GFS accepts no responsibility for the loss of power banks or devices that are left unattended when charging.

10. Cyber-bullying

This involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others. Students will be held accountable for cyber bullying at GFS and any such interactivity that may impact negatively on the learning environment. Students are taught about e-safety and cyberbullying at GFS as part of the computing curriculum.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts messages or calls on mobile phones;
- The use of mobile phone cameras to cause distress, fear or humiliation;
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites;
- Using e-mail to message others;
- Hijacking/cloning e-mail and other social media accounts;
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Snapchat, Twitter, Instagram, YouTube, Ratemyteacher, etc.

In some cases, these types of bullying or defamation can be a criminal offense.

Prevention of Cyberbullying

At GFS, we have clear prevention strategies including:

- Dedicated members of staff oversee the practices and procedures outlined in this policy and monitor their effectiveness.
- Identification of signs of cyberbullying will be shared with staff and the Online Safeguarding Team.
- Pupils will be informed and taught about the risks and internet safety through our E-safety lessons, digital safety framework and pastoral activities.
- Child Protection training by dedicated members of staff will include cyber bullying identification and what to do.
- Positive use of digital technology will be promoted throughout the school and reviewed and monitored by the Digital Curriculum Leaders.
- Partnerships between home and school to encourage clear communication.

Guidance for Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone. Should you need to take the phone or device from a student, the device should be properly sanitised before taking it from the student and before giving it back to the student.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names;
- Make a transcript of a spoken message, again record date, times and names.
- Tell the pupil to save the message/image.
- Go with the pupil and see a member of the Senior Leadership Team (SLT).

Photographs and Images

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Pupils may only use cameras or any mobile electronic device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- Staff may request to see images stored on mobile phones and / or cameras if they have reason to believe that there may be images which contravene school rules. All pupils must allow staff access to images and must delete the images if requested to do so by staff.
- Posting offensive images on any form of social media or website, including YouTube, is a serious breach of discipline and will result in disciplinary action, regardless of the source of the material.

Computers

- Ask the pupil to bring on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you arrange all pages in the correct order and that there are no omissions.
- Accompany the pupil, taking the offending material, to see a member of the SLT.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Guidance for students

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, your Head of Year, your class teacher or a member of the SLT.

- Do not answer abusive messages but log and report them;
- Do not delete anything until it has been shown to your Form/Class Teacher, Parents/guardian or the Head of Year (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.

Guidance for parents

It is vital that parents and GFS work together to ensure that all pupils are aware of the consequences of getting involved in anything that might be seen to be cyber-bullying.

- Parents can help by making sure their child understands the school's policy and above all, how seriously GFS takes incidents of cyber-bullying.
- Parents should also explain to their child/children, the legal issues relating to cyberbullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if needs be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact a member of the SLT as soon as possible. A meeting can then be arranged with relevant members of staff.

11. E-safety at Home

- Get more parental involvement to help with E safety at home and in school.

Advice on the safe use of technologies for teenagers can be found at the following websites:

http://www.whoishostingthis.com/resources/e-safety/
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers
https://www.thinkuknow.co.uk/parents/
http://www.nationalsafetyonline.com

12. Wellbeing

- Encourage parents to help reduce screen-time at home to help improve the wellbeing of their children.
- Monitor what the students are accessing at home.
- Students are only allowed to use the Upstrive app during form time to log how they are feeling. Otherwise, form time is non-screen time for all students.

13. Sanction procedures

Those who misuse digital devices or violate the DDRUA will be subject to disciplinary procedures. Violations may result in disciplinary action up to and including suspension or expulsion for students, when applicable, law enforcement agencies may be involved after consultation with the KHDA.

First incident of misuse:

- If a pupil is found to be using a digital device in an unauthorised manner and during the school day and is seen as a minor violation the pupil may have their network rights removed and may be subject to further disciplinary action. The school reserves the right to remove network access at any time.
- If the pupil is found to be using a digital device in an unauthorised and it is seen as a moderate violation. Parents will be contacted and will be issued with a National Online Safety course which parents and pupils are expected to complete together and sign a document to show they done so.
- A quiz (based on our DDRUA policy) will be allocated to the student and they must pass with above a particular percentage before they are allowed to use their device in school again.

Second incident of misuse:

- Second attempt will result in an immediate internet ban on the account. Parents will be contacted and will be explained that any further inappropriate activity may result in a permanent internet ban. This will be based on the incident itself and the severity of the issue. If considered appropriate 2 week ban or longer.

Third incident of misuse:

- Should the pupil misuse for the third time permanent block of access to the internet will be put in place.

The school takes its responsibilities in relation to digital safety and use of technology by staff, students, parents and visitors seriously and understands the importance of monitoring, evaluating and reviewing its policies and procedures regularly. The school may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

14. Security of Digital Devices

Students shall be personally and solely responsible for the security of any digital devices they bring onsite to GFS. GFS shall not be liable in the event of any theft, loss or damage to such digital devices. Students are expected to use their digital devices and online content safely, responsibly, and respectfully, and to comply with GFS's DDRUA policy at all times.

If a student fails to comply with GFS' DDRUA policy, his/her digital device may be temporarily confiscated by a representative of GFS and the student may be subject to disciplinary action in accordance with the Sanctions Procedure in section 14 of the DDRUA policy. In the event a digital device is confiscated, reasonable steps will be taken to log or label and secure the digital device in a safe area and/or where necessary, turn it over to a GFS administrator as soon as reasonably practicable.

The first time a digital device is confiscated, the student may collect it at the Head of Year at the end of the school day. The second incident where a digital device is confiscated, the student's parent and/or legal guardian will be required to collect the digital device at GFS and meet with a GFS representative to discuss the incident.

Other than when a digital device is confiscated, we do not envisage any circumstances where a GFS staff member would handle a student's Digital Device. However, an exception to this may be where a student requests a form of technical assistance from a GFS staff member. In such circumstances, the student's digital device be logged prior to undertaking such assistance and where necessary, stored in a secure location. In the event a student's digital device is lost or damaged while in the possession of GFS' staff member, an incident report will be created and communicated to the parents and/or legal guardians of the student who owns the relevant digital device and where applicable, an insurance claim will be made by GFS with its insurance provider.

15.Monitoring and review

The Principal and Assistant Head Teacher of Enrichment and E-Learning will be responsible for monitoring and reviewing this policy every year. This will be done in line with GEMS policies.

Signed ..... Date .....11 August 2026.....
Whole School Vice Principal

Signed ..... Date .....11 August 2026.....
Associate Principal

Signed ..... Date .....11 August 2026.....
Executive Principal/CEO/Executive Vice President of Education

Student and Parent/Guardian Agreement

Consequences for Violating the Rules:

Non-adherence to the provisions of this DDRUA will result in disciplinary action in accordance with GFS's standard procedures.

- I acknowledge that I am responsible for my actions on my device, in GFS, at home and elsewhere, and for following the specific rules established for the use of the hardware, software, labs and networks throughout GFS and beyond. I understand that failure to do so could result in a loss of technological privileges.

- I agree I should not share my passwords or account details with anyone and will have full responsibility for the use of my account. I will protect the privacy of others by never posting or forwarding their personal details or images without their consent and never logging in as or impersonating others.

- I agree I will not engage in illegal activities on the GFS network or any other digital environment (e.g. plagiarism, bullying, harassment, tampering with hardware, software or documents, vandalism, unauthorized entry destruction of files or deliberate introduction of computer viruses).

- I agree I will obey procedural safeguards to maintain the performance of GFS's network and digital devices.

- I agree I will respect the rights of others, use appropriate language and avoid offensive or inflammatory material. I will bring incidents of offensive or inflammatory material directed to myself or others to the attention of a GFS staff member.

- I agree I will not share, make, or post online personally identifying information about any members of the GFS community without permission (addresses, phone numbers, email addresses, photos, videos, etc.).

- I agree I will access only those resources that are appropriate for GFS and those resources for which I have specific authorisation.

- I agree I will obey copyright laws and license agreements. Text material, music, software and other media that are protected by law.

- I agree I will not install software on GFS's network without permission of the system administrators.

- I agree I understand that system administrators and teachers may access my files during system maintenance or as a directed action.

- I agree that I will use GFS equipment responsibly and with care. Charges related to repair and replacement caused by abuse, misuse, negligence or loss as determined by GFS administration will be the responsibility of the student and his or her parents.

- I agree I accept full responsibility for supervision when my child is using any digital device, whether provided by GFS or by the parents at home or in other non-GFS settings. I understand that there may be fees or costs incurred which are not covered by the warranty due to abuse, negligence, loss or multiple incidences of misuse of the device by my child. In the case of a personal device purchased under a Bring Your Own Device initiative, I understand that I, as the parent, am responsible for insuring the device and for its maintenance and security settings. I can expect GFS to provide appropriate guidance and support in this area.

- I agree violation of this Digital Device Responsible Use Agreement may result in:
  - Loss of GFS provided technology and network privileges
  - Sanctions
  - Monetary reimbursement to GFS or other appropriate sources

By both parents and students signing the DDRUA summary, held on record by my son/daughter's form tutor, I acknowledge that I have thoroughly read and agree to the GEMS Founders School DDRUA. I will instruct my son/daughter regarding the importance of following all the guidelines included in the agreement.

Parent/Guardian	**Student**
Name:	Name: .....
Signed:	Signed: .....
Relationship to child:	Form class: .....
Date:	Date: .....