# DGPS Parent Digital Policy 23-24

**Written by:** Rachael Parums & Darren Frearson

**Motto**
Learning Together, Growing Together

**Vision & Values**
At Dove Green, we are creating a world class British school that promotes a respectful, happy, caring and inclusive community. We strive to prepare all students to become lifelong learners and responsible citizens, ready to meet the challenges of the future. In partnership with families and the wider community, our goal is to create purposeful, enriched opportunities for students that inspire them to become leaders of their own learning and develop the knowledge, critical thinking skills, and character necessary to succeed in an ever-changing world. We are dedicated to providing stimulating learning experiences through an evolving, challenging curriculum, fully reflecting the culture of the UAE and the wider world.

**DGPS Way**
At Dove Green Private School, we are:

**D**etermined learners
**G**lobal thinkers
**P**ositive achievers
**S**triving for success

Last updated: September 2023

Dove Green
PRIVATE SCHOOL

1. BYOD Policy
2. Responsible Usage Policy (Students)
3. Cyberbullying Policy
4. Responsible Usage Email Policy – (KS2, 3 and 4 Students)

# 1) 1:1 BYOD Policy

**Introduction**
DGPS takes digital literacy and safety online of students and staff very seriously. While we want to ensure that we are integrating and supporting the use of digital technology to enhance and support our curriculum, it is important that everyone is aware and can be supportive of the elements in place which keep us all safe. This policy is a home-school agreement. By signing this, you are agreeing to support us as a school with safeguarding all our students.

In this policy, the iPad, Laptop, Android or Tablet will be referred to as "device".
As part of using a school device and/or having a device of your own which you bring to school, we require the following agreement to be in place.

Before using the device in school, students and parents must e-sign copies of the
**Home School Agreement for bringing your own device (BYOD)**

**1. E-Safety**

Our E-Safety Policy is well established, reviewed annually, and is applicable to iPad, Tablets, Laptops and handheld devices (for example, mobile phones) as well as other technology. The guidelines set out in the E-Safety Policy should be followed.

Issues of E-Safety will be addressed through assemblies, tutorials, E-Safety lessons and other curricula activities. We also encourage conversations about E-Safety at home. Staff have the right to look at the content of the device at any time and will undertake spot checks to ensure that they are being used responsibly.

The UAE web filtering system used at school applies to all school devices. The school network restricts content. Students have a network specifically set to allow us to protect them and their devices. Students should not be connected to any other network, including, staff networks, guest and personal mobile hotspot accounts. VPNs must not be applied to the devices which are BYOD, in line with the UAE law prohibiting the use of VPNs.

**2. The Device**

We recommend purchasing a device which is an iPad 6th/7th Gen or above which has 128gb storage. This is to 'future proof' the device and allow use for many years. You can make comparisons of these models to others by visiting: https://www.apple.com/ae/ipad/compare/.

In addition to this, we recommend you invest in a strong cover for the device and compatible headphones. If you have an iPad which is an earlier than the 2018 model, we recommend you upgrade to allow your child uninterrupted access to apps, such as SeeSaw.

Taking Care of the Device
Students are responsible for the general care of their device:

- Food & drink should be kept away from the device, as it may cause damage to the device.
- A clean, soft cloth should be used to clean the screen, no cleansers of any type.
- Cords and cables should be inserted carefully into the device to prevent damage.
- Devices should never be left in an unattended or unsupervised area.
- The devices should not be disassembled or attempted to be repaired.
- Device batteries must be fully charged and ready for school each day.

- Personal chargers for devices should not be brought into school unless they have been checked and marked by IT support to ensure it is safe to use.

Carrying the Device

- The device should always be kept in its protective case.
- Items carried in a bag alongside the device should be limited to avoid too much pressure being put onto it.
- When travelling to/from school, the device should not be taken out of the student's bag.

Screen Care

- The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.
- Do not lean on top of the device when it is open or closed.
- Do not place anything near the device that could put pressure on the screen
- Clean the screen with a soft, dry cloth. Use of harsh chemicals will damage the screen.

Using the Device

- Devices are intended for use at school each day. Lessons will be disrupted if students forget their device or have failed to charge it.
- Students are responsible for bringing the device to school each day unless specifically instructed not to do so by their teacher/s.

**3. Appropriate Use in School**

In Lessons

- Teachers and students will use the devices in lessons, to support and enhance learning. The amount of usage may vary throughout different year groups and subjects. Some lessons/topics may be more suited to the use of new technology than others.
- Teachers have the right to stop a student using their device at any time if the student is being disruptive and/or not on task. This is in line with the DGPS Behaviour Policy.
- Teachers have the right to access and read any messages sent to the device during school hours.

Break/Lunchtimes

- During lunch/break times, students will leave the devices in their classrooms or bags.
- The device should only be used if expressly allowed by the teacher for educational activities, under supervision.

Charging the Device Battery

- Devices must be brought to school each day in a fully charged condition. Students need to charge their devices each evening.

Screensavers and Backgrounds

- Students should have an appropriate screen saver in place as a picture for their background. This should not be something which could cause offence or concern to any other student or teacher.

Home Internet Access

- The device will need to link to your home wireless network, in support of device use at home.
- Web filtering in school will be set to allow UAE content only. We advise that your parental controls and web filtering systems are in place. Advice on this can be requested from the school.
- The device should be used in an open area where you can monitor what your child is doing.
- You should ask your child to show and explain to you how they are using it for learning.
- You should keep the device out of the bedroom when your child is going to bed.

- You could turn off the wireless router at certain times each night to restrict access.
- You must check the device regularly to ensure no unsuitable activity/downloads have occurred.
- You must disable messaging to the device either permanently, or during school hours. Advice on how to do this can be given by the school IT department.

**Parents are responsible for overseeing the use of their child's device at home. Each family has unique dynamics and it is our intention to respect parenting decisions with regard to device use.**

**4. Behaviour and Misuse**

DGPS takes the following very seriously. Students are not allowed to:

- Send, access, upload or download inappropriate materials/apps.
- Give out any personal information, for any reason, over the Internet.
- Use devices to access social media sites.
- Use devices to access websites, apps or materials that are inappropriate for their age.
- Use devices for any illegal activities.
- Use devices when at break or lunch without permission
- Play non-educational games on the device during lessons or at any time during school.
- Add a personal VPN to the device.
- Change settings on the device to deliberately upset or cause concern to others.
- Share images with others as an "airdrop" at inappropriate times
- Involve themselves in any form of cyberbullying or inappropriate communication
- Receive messages or other non school communication on their device during school hours. Doing so will result in investigation by the SLT and other appropriate UAE authorities.

**5. Protecting and Storing the Device**

Device Identification

- Each device should be clearly labelled with the student's name.

Storing your Device

- Students can take their device home every day after school.
- Do not leave the device in a place that is experiencing extreme hot or cold conditions. Extreme heat will damage the device and extreme cold will cause severe screen damage.

Unsupervised Devices

- Under no circumstances should devices be left in unsupervised areas at home or in school.

**6. Personal Safety**

- Remember that it is important to respect the privacy of others
- Photographs, recording of voice/movie should not be taken without permission from the person.
- Students should not store camera images and recordings on the device or anywhere else, without the permission of the person.
- Uploading photographs/movies from the device to online media sharing sites, such as Facebook, YouTube etc. or public space on the internet, is not permitted.

**7. Health and Safety**

- Be aware of posture when using devices.
- When at home, regular breaks should be taken if using the device (please see the Screen Time recommendations for more details).

**8. Loss/Damage of the Device**

- Where possible, we advise that you activate device location services such as "Find my Device". This will help in locating and locking the device.
- If a device is damaged it is the responsibility of the parent/student to repair/replace.

**9. Safeguarding**

- If at any time you have concerns about the activity on a device and/or something you have seen, you are required to report this as soon as possible to a Designated Safeguarding Leads at DGPS – Rachael Parums or Darren Frearson.

**10. Responsible Use & Behaviour Policy**

- Failure to follow the above guidelines will fall under the Behaviour Policy.

# Responsible Usage Policy (Student)

DGPS takes digital literacy and safety online of students and staff very seriously. While we want to ensure that we are integrating and supporting the use of digital technology to enhance and support our curriculum, it is important that everyone is aware and can be supportive of the elements in place which keep us all safe. This policy is a home-school agreement. By signing this you are agreeing to support us as a school with safeguarding all our students.

In this policy, the iPad, Laptop, Android or Tablet will be referred to as "device".

As part of using a school device and/or having a device of your own which you bring to school, we require the following agreement to be in place.

The UAE web filtering system used at school applies to all devices. The school network restricts content. Students have a network specifically set to allow us to protect them and their devices. The student should not be connected to any other network, including, Staff networks, Guest and personal mobile Hotspot accounts.

1. My device will be linked to STUDENT network at DGPS.
2. I will not apply a VPN to my device, in line with the UAE law prohibiting the use of VPNs.
3. I will not access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
4. I am aware that my teachers have the right to stop me using my device at any time if I am being disruptive and/or not on task. This is in-line with the DGPS behaviour policy.
5. I will not send, access, upload or download inappropriate materials/apps.
6. I will be polite and responsible when I communicate with others.
7. I will not give out any personal information, for any reason, over the Internet or face-to-face, except to my parents.
8. I will not use my devices to access social media sites in school.
9. I am aware that photographs, recording of voice and movie must not be taken without the permission of the other person. I am also aware I must not store camera images and recordings on the device or anywhere else, without the permission of the person.
10. I know that I am responsible for the general care of my device.
11. I know that my devices should never be left in an unattended or in an unsupervised area.
12. It is my responsibility to ensure batteries are fully charged and ready for school each day.
13. I know that my personal chargers for devices should not be brought into school unless they have been checked and marked by IT support to ensure it is safe to use.

14. I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

Note to parents about home use:
Parents are responsible for overseeing the use of their child's device at home. Each family has unique dynamics and it is our intention to respect parenting decisions with regard to the use of the device. If at any time you have concerns about the activity on a device and/or something you have seen, you are required to report this as soon as possible to a Designated Safeguarding Lead – Rachael Parums or Darren Frearson.

Web filtering in school will be set to allow UAE content only. We would advise that you ensure your parental controls and web filtering systems are in place. Advice on this can be requested from the school.

Staff have the right to look at the content of the device at any time and will undertake spot checks to ensure that they are being used responsibly.

# Cyberbullying Policy

**1. Introduction**

DGPS believes that all people in our community have the right to teach and learn in a supportive, caring and safe environment without fear of being bullied that includes parents, staff and children. We believe that every individual in school has a duty to report an incident of bullying or unkindness whether it happens to themselves or to another person. FS and Primary children are not allowed mobile phones in school. Pupils must comply with the expectations outlined in the school Behaviour Policy.

If we find that a child's wellbeing is compromised by cyber-bullying, we will take immediate and effective action. This may mean contacting other parents if we find their son or daughter is involved. We endeavour to foster positive communications with parents, staff and students about their digital lives to ensure that everyone feels supported and able to speak out if they have any concerns.

1.1 What is Cyber Bullying?
Cyberbullying is the use of digital-communication tools, particularly mobile phones and the Internet, deliberately to upset, hurt or be unkind to someone else or a group of people. Technology allows the user to bully or be unkind anonymously from an unknown location, 24 hours a day, 7 days a week. Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher, but it is highly intrusive and can cause emotional distress if not dealt with.

There are many types of cyber-bullying and, although there may be some of which we are unaware, here are the more common forms:

1. **Text messages** —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
2. **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
3. **Mobile phone calls** — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
4. **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
5. **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based chatroom.
6. **Instant messaging** (IM) — unpleasant messages sent while children conduct real-time conversations online using Snapchat, FB Messenger, WhatsApp, Skype or Yahoo Chat – amongst others. It can also be a group chat or 1:1 setting.

7. **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo, Twitter, Instagram and Facebook – although there are others.

**2. DGS Procedures:**
At DGPS, we take this form of bullying as seriously as all other types of bullying and, therefore, will deal with each situation individually. In cases of cyber-bulling, as with all bullying and unkindness, the procedure will fall under the anti-bullying policy. Pupils are taught within their Computing and Moral Education lessons, as well as Assemblies, how to:

- Use internet and technology safely and know about the risks and consequences of misusing them
- Know what to do if they or someone they know are being cyber-bullied or are experiencing unkindness in the digital "world".
- Appreciate the upset and unhappiness that cyberbullying causes.
- Report any problems with cyberbullying or unkindness in the digital world.

2.1 DGPS:

- Has a Responsible Use Policy & Email Policy for pupils that includes clear statements about e-communications and behaviour – a new one will be issued to all pupils to sign in September 2022
- Uses a variety of security and safeguarding tools to ensure that the programs and websites most frequently used for cyber-bullying are unavailable on the school network.
- Provides information for parents on e-communication standards and practices in schools, what to do if problems arise and what is being taught in the curriculum where and when required
- Gives support for parents and pupils if cyber-bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence.
- Has a clear disciplinary framework for dealing with any behavioural issues involving unkindness within the digital world. Once the person responsible for cyber-bullying has been identified, the school will take steps to change their attitude and behaviour as well as ensuring access to any support that is needed.

2.2 Advice to pupils who are victims of cyber-bullying or unkindness digitally:

- Remember: bullying and unkindness is never your fault. It can be stopped & it can usually be traced.
- Don't ignore the bullying or unkindness. Tell someone you trust, such as a teacher, parent or friend. Your teacher, Head of Year or Headteacher will be especially well-placed to help you.
- Try to keep calm. Don't retaliate or return the message. If you show that you are angry, it will only make the person bullying you more likely to continue.
- Do not give out your personal details online including information about where you live, the school you go to, your email address, phone number or social media details etc.
- Keep and save any unkind emails, text messages or images. Then these can be used as evidence.
- If students are bullied online, they should never respond or retaliate to cyberbullying incidents.
- Students and staff should report incidents appropriately and seek support from your teacher, or in the instance of staff, your line manager or SLT staff.
- Save evidence of the abuse; take screenprints of messages or web pages & record the time/date.

Depending on the severity, in the first instance we would request that the person removes the offending comments. If they refuse, we could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies. If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, The school will consider contacting the police. Online harassment is a crime.

There's plenty of online advice on how to react to cyberbullying. For example:
www.kidscape.org
www.thinkuknow.co.uk
www.wiredsafety.org

2.3 Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. If the bullying or unkindness persists, you can change your phone number. Some services or phones allow you to 'block' messages from a sender.

Don't reply to abusive or worrying text or video messages. Don't delete messages from cyberbullies. You don't have to read them, but keep them as evidence. If the calls are simply annoying, tell a teacher or parent. If they are threatening or malicious & they persist, you must pass it on to your parent or teacher.

2.4 Phone calls

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

- Always tell someone else: a teacher or parent.
- Be careful to whom you give personal information such as your phone number
- If you have a mobile phone, make sure you set it to lock down after 20 seconds of not being used – then others cannot use your phone to send message

2.5 Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence and tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) if required.
- Never reply to someone you don't know, even if there's an option to 'unsubscribe' - Replying simply confirms your email address as a real one.

2.6 Web bullying

If the bullying is on a website or social media site (e.g. Facebook) tell a teacher or parent, just as you would if the bullying were face-to-face, even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature.

2.7 Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. Don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or a teacher if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.

**3. FS-Year 1 Addendum**

For children in Foundation Stage and Year 1, not all of this policy is relevant as they have limited access to technology and social media, however, their understanding of the importance of 'stranger danger' and general rules for kindness are all referred to here and acknowledged through inclusion in our PSED/PSHE lessons alongside our general pastoral approach as well as specifically in Computing lessons.

**4. Staff**

In the instance of having a bullying case reported, you should follow procedures set out for any other behaviour instance and report it immediately.

# Responsible Usage Email Policy (KS2/KS3 / KS4 Students)

**1. Introduction**

Use of internet and email services by DGPS pupils is permitted, and indeed encouraged, where such use supports academic progress, in line with the goals and objectives of the school. DGPS acceptable use policy requires that pupils:

- Use email in an acceptable way
- Do not create unnecessary risk to the school and themselves by their misuse of the internet
- Comply with current legislation

**2. Responsible Use**

- Internet access must be in support of educational activities
- All internet access must be via the Student wireless network
- When using email, extreme caution must always be taken in revealing any information of a personal nature.
- Network accounts are to be used only by the authorised owner of the account for the authorised purpose.
- Pupils to exhibit exemplary behaviour on the network as representatives of the school and community. Be polite!

**3. Unacceptable Usage**

- Accessing the Staff and Guest wireless networks to bypass security measures
- Use of personal communications systems in school, for activities that are illegal or against UAE customs, including the use of VPN software
- Use of school communications systems for sending chain letters
- Distributing, accessing or storing images, text or materials that might be considered indecent, inappropriate, pornographic, obscene or illegal
- Distributing, accessing or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying
- Accessing copyrighted information in a way that violates the copyright
- Breaking into the school's or another organisation's system or unauthorised use of a password/mailbox
- Broadcasting unsolicited personal views on social, political, religious/non-school related matters
- Transmitting unsolicited commercial or advertising material (SPAM)
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the school network
- Accessing another person's email account
- Sharing passwords with other students
- Downloading media files for personal entertainment

**4. Use of School Media Resources**

For some activities pupils will require access to school media resources that are saved on the school network. These resources will be controlled by the member of staff leading the activity and the pupils will only have access through a school device. Pupils are only permitted to use these resources for the purpose they were intended to be used for.

They should not:

- take copies of school-owned photos home or store them on their own devices
- post them on social media
- alter the resources

**5. Procedure**

5.1 <u>Stage 1: Preventative measures</u>

Designed to discourage unacceptable usage and to promote positive usage:

- Staff training through insets and CPD - awareness of the risk & indications of unacceptable usage
- Banning of mobile phones during the school day. Senior school pupils are permitted to use mobile phones after 3:15pm, as long as they are outside the school building
- Promoting e-safety amongst the school community
- Assemblies and awareness days
- Monitoring and reviewing of policies
- Effective monitoring of pupil usage

5.2 Stage 2: Sanctions

Sanctions are dependent upon the severity of the offence and consideration of any previous episodes of misuse. The following should be used as a guideline:

1. Verbal warning
2. Head of Year meeting
3. Senior leadership meeting
4. Letter home to parents
5. Controlled use of devices by staff

N.B. All incidents are recorded as a pastoral note by SLT.

**6.Monitoring**

In the interests of Child Safety and Safeguarding, DGPS maintains the right to inspect all school-issued email accounts. Such monitoring is for legitimate purposes only and is documented.

As part of the school's IT programme, pupils are given supervised access to the internet through school computers and the Student wireless network. Use of the internet is subject to both the parent and pupil signed acceptance of the terms of this policy, which is outlined on the final page of this document.

Access to the internet enables pupils to explore libraries, databases, and bulletin boards while exchanging messages with other internet users throughout the world. Families should be warned that some material accessible via the internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

At DGPS, the use of modern firewalls and anti-spam services ensures a high level of network security, in order to combat unsolicited emails and internet content. With internet access comes the responsibility of the user to only access materials that are considered educational in value in the context of the school setting. DGPS staff will make every effort to guide students in the correct use of the internet. As part of this provision, our access is filtered to exclude inappropriate material; however, on a global scale, it is impossible to control all materials. It is imperative therefore, that users be held accountable for their use of the technology.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

**Signed:**

**Print Name:** Christopher Seeley

**Designation:** Principal DGPS

**Date:** September 2023

**Next Review:** September 2024