DGPS Digital Policy 23-24

Written by: Rachael Parums and 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:

Determined learners
Global thinkers
Positive achievers
Striving for success

Last updated: September 2022

Dove Green
PRIVATE SCHOOL

1. BYOD Policy (Y2-6)
2. BYOD Policy (Y7-10)
3. Shared device Care and Responsible Usage Policy
4. Responsible Usage Policy for Internal contractors
5. Responsible Usage Policy - Primary Students
6. Responsible Usage Policy - Secondary Students
7. Responsible Usage Policy - Staff
8. E-Safety Policy
9. Screen Time Policy
10. Cyberbullying Policy
11. Accessibility Policy
12. Responsible Usage Email Policy - KS2, 3 and 4 Students
13. Responsible Usage Email Policy - Staff
14. Remote & Online Learning Safeguarding Policy - Staff
15. Remote & Online Learning Safeguarding Policy - Parents
16. Remote & Online Learning - Safeguarding for Students (Years 2-10)
17. Social Media in School
18. Online Safeguarding Training Expectations (inc. Admin & TA support)
19. Useful Contacts UAE & UK

1.1) 1:1 BYOD Policy (Y2-6)

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 s chool, 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 Lead at DGPS – Rachael Parums or Darren Frearson.

10. Responsible Use & Behaviour Policy

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

1.2) 1:1 BYOD Policy (Y7-10)

Introduction

DGPSS 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.

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.

For the purposes of the secondary school a mobile phone is not an acceptable device. In line with current policy mobile phones should not be visible by secondarystudents during the school day 07:40 – 15:15 unless with explicit permission.

1.2.1 E-Safety

Our E-Safety Policy is well established, reviewed annually, and is applicable devices as well as other technology connected to our network. The guidelines set out in the E-Safety Policy should be always followed.

Issues of E-Safety will be addressed through assemblies, tutorials, E-Safety lessons and other curricular 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 networks, 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 to bypass restrictions or restricted websites.

1.2.2 The Device

or the secondary school we support the use of a tablet however, a laptop is preferred as many websites and applications, that support learning across the secondary school may not function correctly on tablet devices.

Taking Care of the Device

Students are responsible for the general care of their device: When not in use students can store their device in their locker space.

- Food & drink should be kept away from the device, as it may cause damage to the device.
- Cords and cables should be inserted carefully into the device to prevent damage.
- Devices should never be left in an unattended or unsupervised area.

- Device batteries should be fully charged and ready for school each day. However, please ensure the correct charging cable is also available should the need arise.

1.2.3 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.

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.
- 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.
- Device should be used in an open area where you can monitor what your son/daughter is doing.
- You should ask your son/daughter 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.

1.2.4. Behaviour and Misuse

DGPSS 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 without explicit permission.
- 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 and within an appropriate area
- Play non-educational games on the device during lessons or at any time during school without permission.
- Add a personal VPN to the device, with the intent to bypass restrictions
- 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 may result in investigation by the SLT and other appropriate UAE authorities.

1.2.5 Protecting and Storing the Device

Device Identification

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

Storing your Device

- Students should 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 in any area

1.2.6. 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. This is illegal in the UAE and can have serious criminal implications.
- Students should not post or store camera images and recordings on their device or anywhere else, without the permission of the person or the school.
- 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 without explicit written permission.

1.2.7. 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.

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 Lead at DGPS – Rachael Parums or Darren Frearson.

10. Responsible Use & Behaviour Policy
- Failure to follow the above guidelines will fall under the Behaviour Policy.
- Persistent failure to adhere to guidelines will result in device privileges being revoked at school.

Shared iPads Care & Responsible Use Policy

This policy is relevant to Foundation Stage-YR1 Students. Devices should not be used for extended periods of time and all activities should be considered in line with the Screen Time Policy.

Due to the age of the students who are using these devices, the responsible usage will be monitored by the Teachers and LSAs in the classroom. School iPads cannot be connected to iTunes, ensuring content (movies, photos etc.) cannot be downloaded.

Device Care
- Devices should be used for educational purposes only during school hours
- Devices should never be left unattended
- Devices should be returned to the charging unit at the end of their use
- Always place the Device on a stable surface to use it
- Keep all food and drinks away from the Devices

Student should be taught to:
- Use the Device camera to take, forward or pictures or movies for educational activities.
- Always ask permission when taking a photograph or video
- Only navigate apps or websites that have been shared with them

- Take care of the device, not removing the cover or intentionally damaging, placing stickers, writing, drawing on or otherwise defacing the device or case.

Responsible Usage for Contractor Network Access

RUP additional for internal contractors only.
The information below is in addition to the RUP for DGPS staff, for any contractor who works for the school but without a school deployed device must follow all guidelines set out in the Responsible Usage Policy. The below information supersedes any which it may contradict within the staff RUP.

Internal contractors will have limited access to the school network. Staff will have to log into the school's Identity Services Engine and school firewall ensuring that they are verified. Internal contractors should only log into the school's network with official DGPS accounts which will be provided to them.

Internal contractors are not permitted to:
- Take photographs or students or with students under any circumstances (except the schools' photographer).
- Be friends with students online or outside of the school grounds
- Download documentation from the CAD systems which is not directly linked to their job role or employment.
- Download, print or use the system for personal use or gains.

Please note:
DGPS Secondary Leadership Team 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.

Responsible Usage Policy (Primary Students)

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.

Responsible Usage Policy (Secondary Students)

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 to bypass restrictions.
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 personal 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 and I have the correct charger available.
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 or school platforms (examples would be cyber-bullying, use of images or personal information, Misuse of Teams).

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.

Responsible Usage Policy (Staff)

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.

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. Staff have a network specifically set to allow protection of themselves and their devices.

1. My device will be linked to STAFF network at DGPS
2. 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.
3. I am aware that DGPS has the right to stop me using my device at any time if they feel it is not in line with the responsible usage policy.
4. I will not send, access, upload or download inappropriate materials/apps.
5. I will be polite and responsible when I communicate with others.
6. I will not give out any personal information, for any reason, over the Internet or in face-to-face.
7. I will not use my devices to access personal social media sites during the school day.
8. 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.

9. I am aware of the students in my care who are not able to be photographed.
10. I am aware that sharing of images outside the school is not permitted, that photographs should only be shared with other DGPS staff and only if it is for educational purposes.
11. I am aware that Images should not be stored on personal devices, these should be moved to a school monitored platform such as teams as soon as possible.
12. Sharing on agreed public forums which are used to promote the school's positive ethos are allowed where all students pictured have photo consent.
13. I know that I am responsible for the general care of my device.
14. I know that my devices should never be left in an unattended or unsupervised area.
15. 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/where they involve my membership of the school community or school platform (e.g. cyber-bullying, use of images or personal information. Adults can be victims of cyberbullying & this should be reported immediately).
16. Avoid syncing or leaving personal accounts logged into work devices.

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 school DSL – Rachael Parums or Darren Frearson.

Please note:
DGPS Senior Leadership Team or IT Team have the right to look at the content of any school device at any time and may undertake spot checks to ensure that they are being used responsibly.

E-Safety Policy

Introduction
E- Safety at DGPS is defined as safeguarding children in the digital world. The digital world is rapidly growing and changing and with that we need to ensure as a school we also safeguard children when online. DGPS ensures that children are safeguarded in the digital world through a range of preventative measures. Children will be part of this digital world for all of their lives and throughout their educational journey and it is important that as a school we have systems in place to ensure children are protected and know how to keep themselves safe when exploring such a diverse and evolving area.

"The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into 3 areas of risk:

- ***content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;*
- ***contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and*

- ***conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying." (Keeping Children Safe in Education, 2022)*

1. What we do as a school

1.1 The Curriculum

- Class Teachers take E-Safety seriously and as such have mapped out the Computing curriculum carefully to include all aspects.
- All pupils in Year 1 receive age appropriate input regarding their e-safety and their online activity from the Common Sense Media Curriculum.
- All pupils are to create a Digital Charter on completion of their Digital Citizenship lessons (Common Sense Media Curriculum)
- All pupils from Y2-Y10 and above receive detailed input on the following:
    - Maintaining a healthy online presence
    - Strategies for staying safe online
    - What to do if uncomfortable online
    - How to support peers who run into difficulties online
    - Implications of being digital natives - growing up with the internet
    - Digital Footprint Awareness
- Y5 – Y10 also receive detailed input on the following:
    - Impact of online presence and behavior on future employment
    - UAE laws for social media and what can happen if online posts are deemed unacceptable

- The Computing scheme of work has been redesigned to include activities where pupils prepare material in lessons, ensuring that everyday is a safer internet day. Computing lessons for Y1-Y6 will be delivered from the **Code.org** scheme of work.
- Every term, the school will share a focus on e-safety from the Common Sense Education Curriculum and Student Digital Leaders will lead assemblies through role play, shared posters, presentations and student lead innovations.
- There is a Responsible Use Policy / Digital Charter which all pupils must sign. This includes what pupils are permitted to do when logged into the school's network and what to do to continue to remain safe.
- The BYOD scheme (YR2-YR10) has been implemented with safeguards. parents and pupils understand that while logged into the school's network, their online activity may be monitored for their own safety.
- The School runs parental workshops throughout the year to keep the communication channels open on the topic of e-safety.

1.2 Digital Co-curricular Activities

- All co-curricular activities are an extension of the curriculum and subsequently the curriculum policy is followed during co-curricular activities.
- In addition to this, some activities will require pupils to access media resources from 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. This forms part of the Responsible Use Policy which all pupils have to sign.

2. Monitoring Systems

Network access is controlled by Aruba WiFi Controller, and Aruba Core Switch, All BYOD devices are identified and moved into the correct access level. Internet access is controlled by the Fortigate firewall which identifies users and directed to the correct internet and access permissions. Access to unsuitable content is blocked, based on the following:

- Website categories, such as violence, games, social media, adult content, extremism
- Application categories, such as VPN clients, online games, communications/social media software

Activity is logged and available to SLT staff for investigation if required. Under no circumstances are pupils permitted to move between permissions blocks and these are controlled using the user accounts to add a further layer of security.

2.1 Future Digital Safeguarding

When working on school windows computers, pupil activity will be monitored by a software agent which tracks keystrokes and on-screen text against a database of trigger words and phrases. Matches are logged in the database along with a screenshot, for investigation by SLT staff.

The database is designed to pre-warn staff of bullying, self-harm, depression, profanity, extremism, violence and other areas of interest with regard to Safeguarding. Due to the intrusive nature of the programme, it is not currently installed onto pupil-owned laptops.

3 Pastoral Processes

At DGPS we also ensure our pastoral systems include safeguarding children in the digital world and E-Safety is covered through our Moral Education Curriculum, as well as through school systems and procedures. We have regular weekly slots for key stage and whole-school assemblies if this topic needs to be approached or spoken about as a preventative measure. We also hold parent workshops each year, focusing on the digital world and how parents can support and protect their children at home as well as find out about what is happening in school.

Screen Time Policy

Executive Summary

The aims of this document are to:

- Teach students to use their online devices safely, sensibly and healthily to support their learning.
- Support & inform parents about sensible practice, particularly relating to screen time/safe usage.
- Outline to staff, parents & students the things their devices can do to support their learning.
- Outline what resources are available for online learning.

Screen Time Policy

As a school, which actively promote the daily use of devices. Our screen time policy is a necessity required to be supported by all staff, parents and stakeholders of our school.

This policy covers both in school procedures as well as guidance and support to parents at home. The combination of both of these elements will ensure that device screen use is kept relevant and to a minimum for the students' age range.

The school policy is written in line with up-to-date research and digital pedagogy reflected throughout. Above all, it takes into consideration the needs of our students; not only readying them to be part of a digital world but to make sure their individual needs are met. We will also ensure that additional uses such as accessibility features are enabled for those who need to utilise the device to support their special educational needs.

This Policy is supported by The American Academy of Paediatrics (AAP), which encourages parents to help their children develop healthy media use habits early on.

- For children ages 2 to 5 years, *(DGPS Admits students from FS1, ages 3+)* limit screen use to 1 hour per day of high-quality programs.
- At home, parents should co-view online learning with their children to help them understand what they are seeing and apply it to the world around them.
- For children aged 6 and older, place consistent limits on the time spent using media, and the types of media, and make sure media does not take the place of adequate sleep, physical activity and other behaviours essential to health.
- Designate media-free times together, such as dinner or driving, as well as media-free locations at home, such as bedrooms.
- Have ongoing communication about online citizenship and safety, including treating others with respect online and offline.

In School
Lessons are between 20 minutes and 1 hour in length, from a range of subjects, some of which require a more frequent use of technology. Within class time, device work is embedded into the curriculum to support and enhance the learning. Students are monitored and supported in their use of the technology in the classroom and use it to showcase their learning.

The range of learning can be broken down across the curriculum and year groups. Across the school, screen time limits differ due to age and educational needs (Research taken from AAP 2016).

Exceptions to Routine
Students take part in online assessments, e.g. GL assessments. When this does occur, students will be given regular rest breaks. Students with special educational needs will have additional support and time from the inclusion team and/or LSAs. All assessments are age-related and should not exceed the recommended daily screen time.

School Screen Time
Y2 – Y10:
Pupils have access to the following in school time:

- Interactive white board / Portable Learning Screens
- School laptops
- Own device

Independent learning and activities for each year-groups are differentiated by depth-of-skill. Screen time is recommended at the same level; pupils in Years 5-10 would be required to complete more independent learning to support the skills which they are learning in class.

Elements of this would be:

- Researching on reputable websites for content
- Finding sources of work, images or videos to support their work
- Developing individual pieces of work which supports their concepts and learning of a subject.
- Working as a group to develop presentations.
- Transferring written work to programmes on their device to present in a different format.

Screen time in the Primary School is restricted, but not limited to the use of:

- Pupils will not use a device for longer than 30 minutes at one time, e.g. reading a book or using an app in conjunction with another learning activity .
- Coding games, which are used to consolidate learning or introduce new concepts of computer science and coding.
- Interactive white board sessions for small groups or whole class activities.
- Pupils use programmes and software on the Device for digital skills e.g. writing, researching and/or formative and summative assessments.
- Learning Apps in conjunction with lesson input or extension activities, e.g., TT Rockstars and/or I Read Arabic and/or I Start Arabic.
- iMovie, Clips and PicCollage to collate, review and showcase learning.
- Lessons of such will include regular checks on progress to ensure students are not looking at the screen for long periods of time.

Safeguarding your Child
You can track and monitor students device usage via a range of platforms on built in software to support positive screen time such as:

Apple - https://support.apple.com/en-us/HT208982
Google Play - Apps - https://play.google.com/store/apps/details?id=com.screentime.rc&hl=en
Google - https://support.google.com/families/answer/7103340?hl=en
Common Sense Media - https://www.commonsensemedia.org/screen-time

National Online Safety

If you would like to know more about Online Safety and the Digital World Click here for our parent resources and online courses - https://nationalonlinesafety.com/enrol/DGPS-abu-dhabi

Interactive Digital Media
DGPS supports the use of meaningful and age appropriate interactive digital media. Applications which are added to the students iPad are researched prior to use for content and educational purpose.

E-books
Interactive digital books are used as part of the DGPS curriculum. The use of this form of digital media is used as a relevant form of 21st Century learning. Research shows this form of learning can have an impact upon student comprehension. We will use apps which have comprehension quizzes and/or reflection questions at the end. In addition to this, we would use this media as part of a guided reading group or a 1:1 reading session, to ensure that the student gains understanding of the book's content.

Break / Snack times
During rest breaks, if students are unable to be outside, in order to reduce screen time we suggest that where possible staff play music or an audio book. This will allow students to be supported in cognitive development but without the impact of screen time.

Device Downtime
- Students are not permitted to have their device with them during break and lunch times. This is to reduce the impact of screen time throughout the school day.
- We advise that students put their devices onto airplane mode when studying to allow them to fully focus on their work.
- We advise that students take breaks between learning on a device.

Remote Learning (In case of closure)
In the event of remote learning, students will be given a range of online learning tasks which are specific and measurable to the amount of time which their age range should spend on a device. DGPS will ensure that the platforms which are used for remote learning are specific and meaningful with relevant tasks and objectives mapped out by the year groups and subject specialists to ensure that they are accessing high quality digital material.

SEND
Students at DGPS who are supported additionally for a special educational need or disability have accessibility modes on their devices enhanced. This comes in a variety of ways to support the learner best.

- Enhanced text size
- Speak Screen
- Speak Selection
- Typing Feedback and Predictive Text
- Voice Over: provides auditory reinforcement
- Guided Access: helps to reduce distraction
- Colour Invert
- Colour Filters
- Colour intensit

Digital Safety
As part of the curriculum at DGPS, we ensure that students have restricted access to web content. Social Media is not allowed to be accessed via the school iPad and from student's own devices during the school day. Content on a range of Digital safety is delivered to students across the curriculum via Common Sense Media Education, Google, *BeInternetAwesome* and the pastoral curriculum.

Child Protection
The school reserves the right to report any information provided to school which we feel is inappropriate and/or harmful to a student, to the child protection service.

This may include:

- Excessive screen time allowances
- Unsupervised access to inappropriate content

Home Screen Time
As a school we highly recommend that students are supported at home when using their device either by learning together as a parent and child, talking through content or for older students reviewing and questioning elements of the learning which they have been completing.

We support parents in the creation and use of device monitoring at home on all device management platforms. As a school we do not advocate the use of apps which are not age appropriate and recommend only applications and websites which are suitable and meaningful.

We advise parents to have open communications with their children about their device use and screen time allowances to ensure that they are safe on the internet at home.

All information and research from the DGPS Screen Time policy is from the American Association of Paediatrics reports on the following:

- Children and Adolescents and Digital Media - http://pediatrics.aappublications.org/content/138/5/e20162593
- Media Use in School-Aged Children and Adolescents - http://pediatrics.aappublications.org/content/138/5/e20162592
- American Academy of Pediatrics Announces New Recommendations for Children's Media Use https://www.aap.org/en-us/about-the-aap/aap-press-room/Pages/American-Academy-of-Pediatrics-Announces-New-Recommendations-for-Childrens-Media-Use.aspx
- Media and Young Minds - http://pediatrics.aappublications.org/content/138/5/e20162591
- Screen Time: Advice for Parents - https://www.webwise.ie/parents/screen-time-advice-for-parents/

Cyberbullying Policy

(To be read in conjunction with the Anti-Bullying 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.

Accessibility Policy

Students with accessibility issues include a wide spectrum of disabilities. Whilst these disabilities cannot be compared directly, SENDA legislation (HMSO, 2001) enforces the remit of accessible design for all students, and this policy is to be a representation of the composition of students with accessibility issues in any given cohort.

SEND
All students at school have access to all the accessibility features of the Apple devices, however all students who have a recognised SEND need will have support to adapt their personal device to suit their needs.

Mobility:
- Speech-to-text transcription
- Text editing
- Comprehensive navigation
- Voice Gestures
- Attention awareness
- On-device processing for privacy

Vision:
- Display & text size: Contrast, tone, Brightness, Enlarged text
- Braille Commands with voiceover
- Screen curtain (privacy)
- Live listen
- Closed captions and subtitles
- Voice controls
- Switch controls
- Assistive touch
- Reduce Motion

Hearing & Voice Control:
- Hearing aid connection
- Dictation
- Swipe to type
- Speech Selection

Learning:
- Quick access dictionary
- Safari Reader: Greater Clarity
- Guided Access
- Screen time controls
- Siri

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 Stage 1: Preventative measures

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. Secondary 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.

7. Agreement for Acceptable Use of School Email and Internet Services

Pupil

As a user of the school's internet and email services, I agree to comply with the school rules on its use. I will use these systems in a responsible way and observe all the restrictions explained to me by the school.

Pupil Full Name:

Pupil Class:

Pupil Signature Date:

Parent
As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.
Parent Full Name:
Parent Signature Date:

Responsible Usage Email Policy - Staff

Introduction
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. This Responsible Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of IT in their everyday work.
- Staff do not bring themselves or the school into disrepute with their use of personal social media.

The school aims to ensure that staff and volunteers have reliable access to IT to enhance their work, to enhance learning opportunities for pupils and in return, expects staff and volunteers to agree to be responsible users.

DGPS delivers a British curriculum in English, therefore all staff should set their computers to UK English rather than US English, to assist with correct spelling.

Responsible Use Policy Agreement
I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of IT in supporting and enhancing student learning, and I will ensure that students receive opportunities to gain from the use of IT. I will, where possible, educate students in my care in the safe use of IT and embed e-safety in my practice.

For my professional and personal safety:

- I understand that the school will monitor my use of the school's IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems outside of school
- I understand that school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my password to anyone else, nor will I try to use any other person's username and password.
- I will not allow anyone to use my account.
- If I become aware of any illegal, inappropriate or harmful material or incident, I will report it immediately to a member of SLT

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others - I will do so with their permission and in accordance with the school's policy on the use of digital/video images.

- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (laptops, mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to school equipment, or equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- Users must keep their personal social media accounts e.g. Facebook & blogs private and post no information including personal photographs or videos that could bring the school into disrepute. Staff will not participate in chat rooms with pupils or accept 'friend' requests in any form.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

This policy has been drawn up using the recommendations of the South West Grid for Learning (www.swgfl.org.uk)

Remote & Online Learning - Safeguarding Policy (Staff)

During a time where remote learning is introduced please ensure that the following is adhered to. Please ensure this is read along with the school's Safeguarding Policy.

Communication with Pupils

- All set work is on SeeSaw or Teams and is appropriate to the age, ability and is culturally sensitive.
- Do not send an email where the signature includes "From my iPhone/iPad". You must set a professional signature.
- If you are using an iPad or other device it must be linked to a school storage system - e.g. Sharepoint/Google Drive not your own personal accounts. Preferably please use a school device whenever possible - it protects you first and foremost!
- Do not send any form of communication to pupils or parents from your personal accounts.
- Any inappropriate materials, or communication which you feel are of wellbeing or safeguarding concern must be immediately forwarded directly on to a Designated Safeguarding Lead (Rachael Parums or Darren Frearson), or the Principal.
- Pupils who are either not engaging with remote learning or are completing work at unsociable hours must be reported following the agreed communication channels.
- Do not share remote learning information or resources from your school device to any personal accounts.
- Do not communicate with pupils and parents via social media or messaging services.
- Do not post anything which would be deemed negative to the school's reputation, deemed inappropriate or illegal by UAE law.
- Do not post personal activities or statements on social media during remote learning hours.

Forums, pre-recorded videos and live 1:1 communication

- Do not use platforms other than the ones authorized directly by the school. The IT Department should be informed about all the platforms used by teachers at the school.
- Live videoing may occur during the remote learning period to conduct tutorials and smaller groups for lessons.
- The pupils cameras can be activated at the teacher's discretion to promote social interaction and engagement but this is not compulsory. It is up to the teacher if they want to do this. If pupils cameras are activated they must follow the remote learning guidelines. If they behave inappropriately or are not following these guidelines then please ensure they are asked to turn off their camera and terminate the lesson, activity or conversation and follow up with the DSL or a pastoral lead.
- Professional and culturally acceptable dress is required if using pre-recorded videos or live communication during the remote learning period. If you wear a DGPS kit or a set uniform this should be worn for pre-recorded videos and not personal attire.
- Use of language should be professional at all times as you would in a classroom and school environment.

- The environment of which the video is being recorded or is conducted live must be appropriate ensuring nothing is personally identifiable and the background is clear of anything deemed inappropriate. It should look like professional 'space' as much as possible even if being conducted at home.
- Only DGPS staff should be in the videos or the teaching materials created.
- If the communication is live and there are wellbeing or safeguarding concerns the conversation must be immediately terminated and reported to a DSL (Rachael Parums or Darren Frearson).
- Never conduct any form of live communication with only one pupil (unless a parent is also present). If a tutorial is conducted and only one pupil is logged in you must terminate the conversation and come back to it at a later date when more pupils have joined.
- If pupils are communicating negatively or inappropriately during a forum or via written communication of any sort the conversation must be immediately terminated and reported to a DSL (Rachael Parums or Darren Frearson).
- If pupils are dressed inappropriately during a video or picture which they post onto the platforms this should be reported to the pastoral team who can make a decision whether this then needs to be escalated to the DSL.
- Please check all pre-recorded videos with a line manager or someone in your department for checking and monitoring purposes (if applicable).

Remote & Online Learning - Safeguarding Guidelines for Parents

During a time where remote learning is enforced, please ensure that the following is adhered to and discussed with your child as a joint agreement. Please note this document may change due to fluidity of the remote learning process.

Communications with DGPS staff

- If your child is communicating with staff the language used should always be professional and appropriate.
- Any communication which you feel is of a wellbeing or safeguarding concern must be immediately forwarded to your child's class teacher for further investigation.
- Your child should not be engaging with remote learning or completing work, tasks or activities at unsociable hours.
- Your child should not be communicating with staff via personal messaging services or non- school messaging services.
- Your child should not post or write anything which would be deemed negative to the schools reputation, deemed inappropriate or illegal by UAE law.
- Please ensure that face-to-face communication is only between teachers and pupils. Any parent to teacher communication should be in the usual manner, via email unless discussed beforehand.
- Parents and pupils should not record, share or comment on public forums about individual teachers.

Forums, videos and live 1:1 communication

- When using live communication, remember that this is an extension of the classroom and your child should conduct herself or himself as they would in a classroom or school environment.
- Your child should not use platforms other than the ones authorized by the school directly.
- Professional and culturally acceptable dress is required if using video communication during the remote learning period.
- Use of language should be professional and appropriate at all times.
- The environment of which the communication is filmed or is being recorded must be appropriate ensuring nothing is personally identifiable.
- If the communication is live and there are wellbeing or safeguarding concerns the conversation/video must be immediately terminated and reported directly to the child's tutor or class teacher who will inform the relevant safeguarding or pastoral leads.

- Your child may use their video whilst conducting live communication with staff for lessons or tutorials to promote positive social interaction. Your child does not need to stream their video if they do not wish. If you do not want your child activating their camera at all during the remote learning process please contact his or her tutor directly with formal written communication via email. This excludes Foundation Stage where video communication between school and home must include the parent who would be also present in this communication.
- If your child or their peers are communicating negatively or inappropriately during a forum or via video the conversation/video must and will be immediately terminated and reported via your child's class teacher.
- Your child must be on time for the live lessons, tutorials or activities. The sessions cannot be conducted outside of the stated time decided by the teacher.
- Your child should remain attentive during live sessions and online communications.
- Your child will not be taking part in any live communication lesson, activity or tutorial with only the teacher. An adult from home would be present or another staff member if a live communication lesson, activity or tutorial is conducted with just one pupil.
- Parents or children MUST NOT record any online interactions, lessons, activities or tutorials.
- Your child must ensure they end the session as soon as the teacher indicates for them to do so.
- Your child must always be kind online.

Remote Learning - Safeguarding for Pupils (Years 2-10)

During a time where remote learning is enforced please ensure that the following is understood to ensure the online safety for all. If the below expectations are not followed and you behave inappropriately or are not responsible online, there will be consequences and live communication could be temporarily suspended or terminated. Those children in Years 2-6 must read through the guidelines with an adult at home to ensure they fully understand their responsibility online and the expectations associated with this.

Please note this document may change due to fluidity of the remote learning process.

Live communication expectations

If you are communicating with teachers and or your peers the language used should always be kind and respectful as you would use in the school environment and community. Any worries or concerns online must be immediately forwarded to your parents, an adult at home or your class teacher.

- You should not be engaging with remote learning or completing work, tasks or activities late into the evening or in the early morning outside of school hours.
- You should not be communicating with teachers or any DGPS staff via personal messaging services or non-school messaging services.
- You should not post or write anything which would be deemed negative to the schools reputation, deemed inappropriate or illegal by UAE law.
- You should not record, share or comment on public forums, like social media, about individual teachers, the school or your peers.
- You should only communicate with teachers using the suggested school platforms or using your school email account.
- You should only be using the suggested platforms guided by the school to complete work or conduct school conversations or to access live lessons.
- Live videoing may occur during the remote learning period and if you are able to share your camera you must ensure you are dressed appropriately with cultural sensitivity in mind.

- If your camera is turned on you must ensure you are not in a private space such as your bathroom, but in an open space in your home.
- You must ensure nothing is personable or identifiable in the background if your camera is activated. It should look like neutral 'space' as much as possible even if being conducted at home.
- Only DGPS staff will share videos, teaching materials, activities or lessons for you to use.
- Live communication will never be conducted with only one pupil (unless a parent or another adult is also present). If a live communication begins and only one pupil is logged in the teacher will make you aware and terminate the conversation.
- If your peers or yourself are communicating negatively or inappropriately during a forum, live communication or of any sort the conversation will be immediately terminated and reported. Your parents could also be informed.

Social Media in School

Photography

- Students should sign the agreement annually for photographic consent.
- Students will fall into three categories for photography:
    - Allowed on all streams of school social media & educational platforms
    - Students are allowed to be photographed for academic purposes only
    - Students are not allowed to be photographed for any purposes

As per the Responsible Usage Policy, staff must be logged into their DGPS accounts on their devices to ensure that photographs are not stored in personal clouds. This is for the safety of staff and students.

Teaching staff all have been provided with a device/laptop/desktop to use for teaching and learning in the classroom. Staff will be permitted to use this to photograph students completing tasks and work in the school environment.

Staff should note that this is only permitted due to the device being connected to the school's Teams network and these images should not be transferred onto any other device.

Staff should encourage the students to take photographs of their own work and their own learning experiences to support their understanding of the curriculum.

Photographs of those students who are permitted to be on social media can be shared with the marketing team upon request.

Online Safeguarding Training Policy (including Admin and LSA support)

Online safety in school is of paramount importance, with the introduction of 1:1 devices from Year 2-10, it is important that all staff across the school are aware of how to identify and be aware of the online risks which are facing children and young people.

Due to this, we advise ALL staff to complete the following Online E-Safety Training. Please create a log-in to access the free course:
https://www.commonsense.org/user/login?destination=/education/training/teaching-digital-citizenship%3Fcheck_logged_in%3D1

Courses of interest are as follows:

- The role of safeguarding around SEND and vulnerable learners
- DSL Level 1/2/3 annual certificate in online safety
- Annual Online safety course for ICT Leads
- Annual Online Reputation Course for Schools and Staff
- Certificate in Cyber Security in schools
- Certificate in Data protection & GDPR in Schools

Useful Contacts - UAE

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/child-digital-safety

Signed:

Print Name: Christopher Seeley

Designation: Principal DGPS

Date: September 2023

Next Review: September 2024