JPS Digital Citizenship and Online Safety Policy

Mission statement

An ever-evolving experience for ever-evolving learners.

At GEMS Jumeirah Primary School, we believe that everyone can achieve highly with equitable access to the right opportunities and support. As a high performing school, we recognise and embrace the uniqueness of every child. We create an inclusive, nurturing environment, prioritising the psychological wellbeing of all, allowing children to feel happy, safe and confident. Children at JPS know that anything is possible for them and they aspire to be the best versions of themselves.

We meet the diverse needs of all children and their families to facilitate the best possible individual experience to ensure our learners excel beyond their potential flight path. Our bespoke, innovate curriculum is carefully designed and continually reviewed to:
* Guide learners in developing their values, behaviours and learner competencies to prepare them for success in an ever-evolving world
* Challenge learners and help them to discover their passions, talents and interests
* Provide leadership opportunities for all learners, allowing them to influence the direction of travel for key aspects of school

We are a diverse learning community, passionate about inspiring a love for learning in our children, staff and families. Our inclusive actions and behaviours are led by our core values of Kindness, Empathy, Respect, Hard Work and Resilience. This is clear through our acts of philanthropy and environmental sustainability. The JPS family is proud to lead the way in contributing positively to our local and wider community.

Introduction

> *"In this increasingly global world of information, students must be taught to seek diverse perspectives, gather and use information ethically and use social tools responsibly and safely."*
>
> American Association of School Librarians, Standards for the 21st Century Learner.

A digital citizen therefore knows how to harness the power of technology safely, respectfully and responsibly. A digital citizen is aware of the risks of cyberbullying, knows what to do to prevent it and how to respond to it.

Purpose of policy

At Jumeirah Primary School, we are committed to the wellbeing of all our children and providing a caring, friendly and safe environment so they can learn in a secure atmosphere, while embracing the learning potential of the Internet and digital media. The purpose of this Digital Citizenship and Online Safety policy is to nurture a school ethos where pupils learn to make safe, responsible and respectful choices and to promote a whole school community approach to digital citizenship.

Aims and objectives

- To ensure all members of the school community understand what digital citizenship and online safety is
- To equip all children with the knowledge of how to stay safe online
- To safeguard all children from potentially harmful and inappropriate online material
- To provide a safe and secure environment, where all can learn without anxiety, and measures are in place to reduce the likelihood of inappropriate usage, content and cyberbullying
- To produce a consistent school response to any cyberbullying incidents that may occur
- To promote clear procedures of how incidents of cyberbullying are dealt with

Online Safety

The breadth of issues classified within online safety is considerable and ever-evolving, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

If staff feel pupils, students or staff are at risk, it can be reported to the Anti-Phishing Working Group (https://apwg.org/).

Prevention

The ‘Appropriate Usage of Screens Agreement’ (Appendix A), which outlines expectations for all, is shared with staff, children and parents.

Staff are responsible for creating strong passwords to protect their work accounts. The IT Team and teaching staff support students by providing and maintaining secure passwords. Teachers ensure students learn strategies for managing online information and keeping it secure from online risks.

Filtering and monitoring are essential practices in safeguarding students and staff from illegal, inappropriate and potentially harmful online material, however no filtering system can be 100% effective, therefore, at JPS, children learn how to keep themselves safe online through teaching and learning opportunities, as part of the broad and balanced curriculum.

Filtering

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video. At JPS, security profiles are created in the firewall for traffic of separate user categories (staff, students, guests).

GEMS as a company and JPS as a school have appropriate filtering systems in place on school devices and school networks to block harmful and inappropriate content, without unreasonably impacting teaching and learning or school administration and restricting students from learning how to assess and manage risk themselves.

Monitoring

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring user activity on school devices is an important part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

There are both technical and manual monitoring solutions. For monitoring to be effective, it must pick up incidents that are of concern urgently, usually through alerts or observations, allowing for prompt action.

Manual monitoring

At JPS, children are not permitted to use devices whilst unsupervised. All staff conduct in-person monitoring by circulating the room while students are using devices. This acts as both a deterrent for risk-taking behaviour and allows for prompt intervention where there is cause for concern.

Technical monitoring

Technical monitoring solutions rely on network monitoring and/or software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

Reporting Concerns

The designated safeguarding lead (DSL) is responsible for any safeguarding and child protection matters that are identified through monitoring.

All staff are aware of reporting mechanisms for safeguarding and technical concerns. They immediately report to the DSL (in person and/or through the Guard platform) and IT Team if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics that could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Checks and Documentation

Filtering and monitoring systems at JPS are regularly checked to ensure they are effective and applied to all devices. Checks are conducted when significant changes take place (for example, technology, policy or legislation), in response to incidents and at least annually. These checks are recorded, including details about the location, device and user alongside the result and any associated action.

Resources

At JPS, we have adopted and follow the National College's multi-award winning programme 'National Online Safety'. The goal is to educate and offer tools to teach digital citizenship and online safety to children, parents and educators. This is embedded within our curriculum from Year 1 to Year 6 covering a number of categories:

- **Internet safety**: staying safe while exploring online
- **Privacy and settings**: learning strategies for managing online information and keeping it secure from online risks, creating strong passwords and recognizing scams
- **Digital footprint and reputation**: pupils learn to protect their own privacy and respect others' privacy and learn to self-reflect before they self-reveal
- **Self-image and identity**: helping pupils explore their own digital lives, focusing on their online versus their offline identity. Pupils learn the risks of presenting themselves through different hats and the effects on their sense of self, their reputation and their relationships
- **Relationships and communication**: learn about digital ethics and how to communicate online
- **Cyberbullying**: pupils learn about cyberbullying - what is it, how to prevent it and how to respond to it
- **Information literacy**: learning how to evaluate the quality, credibility and validity of websites and give proper credit
- **Creative credit and copyright**: reflecting on their responsibilities and rights as creators, where they consume, create and share information

Preventing and responding to cyberbullying

What is cyber bullying?

- Cyber bullying includes sending or posting harmful or upsetting text, images or other messages using the internet, mobile phones or other communication technology
- It can take many forms, but can go even further than face-to-face bullying by invading home and personal space and can target one or more people
- It can take place across age groups and target pupils, staff and others
- It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images
- It can include messages intended as jokes, but which have a harmful or upsetting effect

Cyber bullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips via mobile phone
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chat (e.g. during online games)
- Unpleasant messages sent during instant messaging
- Unpleasant or defamatory information posted on social networking sites (e.g. Facebook, Instagram, SnapChat)

Signs and Symptoms

A child may indicate by signs or behaviour that he or she is being cyberbullied. Adults should be aware of these possible signs and they should investigate if a child:

- Changes their usual routine
- Is unwilling to go to school
- Becomes withdrawn anxious, or lacking in confidence
- Becomes aggressive, disruptive or unreasonable
- Begins to do poorly in school work
- Is frightened to say what's wrong
- Is afraid to use the Internet or mobile phone

- Is nervous and jumpy when a cyber message is received
- Is bullying other children or siblings
- Stops eating
- Cries themselves to sleep at night or has nightmares
- Attempts or threatens suicide or runs away

These signs and behaviours could indicate other problems, but cyberbullying should be considered a possibility and should be investigated. This is not an exhaustive list and children may display other behaviours that appear out of their character.

Responding to cyberbullying

A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

- Impact: possibly extensive scale and scope
- Location: the anytime and anywhere nature of cyber bullying
- Anonymity: the person being bullied might not know who the perpetrator is
- Motivation: the perpetrator might not realize that his/her actions are bullying
- Evidence: the subject of the bullying will have evidence of what happened

Support for the person being bullied

As with any form of bullying, support for the child will depend on the circumstances.
Examples include:

- Emotional support and reassurance that it was right to report the incident
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff
- Advice on how to block the bully from future online communication
- Actions, where possible and appropriate, to have offending material removed
- Advice to consider changing email addresses and/or mobile phone numbers
- Discuss contacting the police in cases of suspected illegal content

Investigation

Again, the nature of any investigation will depend on the circumstances. It may include, for example:

- Review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages)
- Efforts to identify the bully, which may include looking at the media, systems and sites used. Witnesses may have useful information
- Requesting a pupil to reveal a message or other phone content or confiscating a phone
- Working with the bully

Work with the bully and any consequences will be determined on an individual basis, with the intention of:

- Helping the child harmed to feel safe again and be assured that the bullying will stop
- Holding the bullies to account, so they recognize the harm caused and do not repeat the behaviour
- Helping bullies to recognize the consequences of their actions and facilitating change in their attitude and behaviour
- Demonstrating that cyber bullying, as any other form of bullying, is unacceptable and that the school takes this extremely seriously.

Roles and responsibilities

The role of Children

- Children are encouraged to tell anybody they trust if they are being cyber bullied, and, if the bullying continues, they must keep on letting people know
- Children must report any incidents that they witness
- Children are encouraged to stand up assertively and safely to a bully and are provided with a range of strategies on how to do this, whether they are being bullied or are a bystander.

The role of Parents

- Parents who are concerned that their child might be being cyber bullied, or who suspect that their child may be the perpetrator of bullying, should contact their child's Class Teacher immediately, who will record the concern and monitor the situation, reporting back to parents as often as needed. The class teacher will inform the Head of Year as well as the Wellbeing Department to offer an effective and collaborative response plan

- Ensure children do not have access to inappropriate websites or online materials, including through the synching of family devices
- Ensure children do not have access to a VPN
- Parents **must not** contact their child during the school day through messenger services on their child's device. Contact should only be made via the teacher or info_jps@gemsedu.com
- Parents have a responsibility to support the school's Digital Citizenship policy, as well as the JPS Appropriate Usage of Screens Agreement, actively encouraging their child to make safe, responsible and respectful choices

The role of the Teacher and Teaching Staff

- All staff in our school take all forms of cyber bullying seriously and seek to prevent it from taking place
- Teachers keep their own records of all incidents that happen in their class and that they are aware of in the school. If a member of staff other than the Class Teacher witnesses or is informed of an act of bullying, they will refer it to the Class Teacher, who then records and investigates
- If any cyber bullying takes place between members of a class, the Teacher will deal with the issue immediately. Class Teachers may choose to deal with incidents through whole class circle time or discussion with the children involved as appropriate. The class teacher will inform parents and will work collaboratively with the Head of Year and the Wellbeing Department
- All members of staff ensure they are aware of the policy so that they are equipped to follow the procedures.

The role of the Wellbeing department

- The Wellbeing department ensures that all staff receive sufficient training in digital citizenship and are equipped to identify and deal with all incidents of cyberbullying
- Support children (victims, bullies and bystanders) through Circle Time and/or individual/group discussions, as necessary, to deal with any incidents of cyberbullying
- Carry out parent workshops to support parents with the many questions and issues that arise with technology
- Keep the Principal, SLT and other relevant staff informed.

The role of the Head of Year

- Ensure time is allocated at the beginning of every team meeting to discuss any vulnerable children or incidents that the team should be aware of that may have occurred throughout the week
- Be aware of any incidents of cyber bullying relevant to their year group and keep the Wellbeing department and other relevant staff informed
- Ensure the Class Teacher is the first point of call and support them, as required.

The role of the Principal and SLT

- It is the responsibility of the Principal and SLT to implement the school Digital Citizenship and Online Safety policy and to ensure that all staff (both teaching and non-teaching) are aware of the school policy and know how to identify and deal with incidents of cyberbullying
- If cyber bullying continues after the involvement of the Wellbeing department and Head of Year, the children involved will be called with their parents to have a meeting with the Principal/member of SLT.

Policy review

This policy has been discussed and agreed by the JPS teaching staff and leadership teams for implementation.

GEMS JUMEIRAH PRIMARY SCHOOL

GEMS EDUCATION

Appendix A

APPROPRIATE USAGE OF SCREENS AGREEMENT

MOBILE PHONES

✓ Mobile phones are **not** allowed. If I need to call home, I can ask my teacher and use the phone at reception

SCREEN USAGE

✓ Screens are used for learning

✓ Screens are used in the classrooms

✓ Screens are used when my teacher asks me and with adult supervision

✓ I do not use a screen in the hallways, in the bathroom, outside, or at break

INTERNET SAFETY

✓ I use the same safety rules online as offline

✓ I only share my passwords with my parents

✓ I don't share any personal information online (phone number, address, school name...)

✓ I use safe search engines: Kidrex and YouTube for kids

✓ I have a parent control app or software on my device to protect me from inappropriate content or usage

✓ I will tell a trusted adult if anything online makes me feel uncomfortable, sad, or unsafe

✓ I will tell a trusted adult if I am a victim of or witness any cyberbullying

✓ I do not have inappropriate games on my device (games rated 12+ on www.commonsensemedia.org)

✓ If I have appropriate games on my device, I keep them for my home usage

DIGITAL CITIZENSHIP

✓ I know that the Internet is a public space; I will respect myself and others online

✓ I will communicate kindly online; I will not tease, embarrass, or bully others

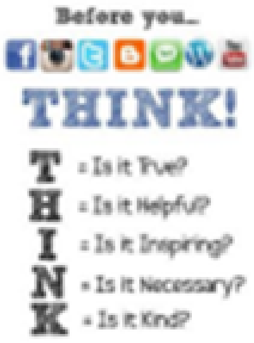
✓ I will learn in school about making safe, responsible, and respectful choices

✓ I know that not everything I read, hear, or see online is true

✓ I will collaborate with my parents so that we can set up rules for going online (when, where, for how long, and on which sites)

✓ I know how to stay balanced with my life and activities offline

OWNERSHIP OF WORK


Before you...

THINK!

T = Is it True?

H = Is it Helpful?

I = Is it Inspiring?

N = Is it Necessary?

K = Is it Kind?

✓ I will create my work with my own words and will not plagiarize from the Internet

SOCIAL MEDIA USAGE

✓ I must be 13 to use social media

✓ Social media usage is not allowed at JPS

✓ If I do use social media outside of school, I must ask permission from the children's parents before posting anything about them (name, picture, video...)

✓ I am accountable in school for any teasing or cyberbullying online

CONSEQUENCE FOR MISUSE

✓ Teachers can inspect my device at any time to make sure I am honouring this agreement

✓ If I do not adhere to this agreement, my device use will be removed

✓ Depending on the severity of my choices, my parents will be called to school