أكاديمية جيمس ولينغتون - شارع الخيل
GEMS Wellington Academy
AL KHAIL

Online Safety Policy

2023-24

Date last reviewed | June 2023
Review period | Annually
Lead Reviewer(s) | Primary & Secondary Vice Principals

"Empowering students to aspire, create and excel in the world that is, so they can help create the world that will be"

The Science of Learning

Social Enterprise

Student Agency and Innovation

Aims and Expectations

This policy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that staff understand their role in supporting online safety

The Four Categories of Risk

The Academy groups wellbeing into three key pillars that link directly to the school vision. Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as fake news, racism, misogyny, self-harm, suicide, antisemitism, sexually offensive material, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them e.g., for criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images and online bullying; and
- **Commerce** – risks such as online illegal financial acts, inappropriate advertising, phishing and/or financial scams

Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the senior leadership team to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students of determination. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Senior Leadership Team

Senior Leaders are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

The DSL and Deputies take lead responsibility for online safety in school, in particular:

- Working with the safeguarding team and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding Policy
- Ensuring that any online safety incidents are logged on Guard and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on Guard and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Ensuring all staff have completed online training, including in-house and GEMS-wide training
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the Leadership Team and/or governing board

This list is not intended to be exhaustive.

The Academy IT Management Team

Our School IT management team is responsible for:

- Putting in place an appropriate level of security protection procedures, in line with GEMS policy, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly, in line with GEMS policy
- Conducting a full security check and monitoring the school's ICT systems on a regular basis, in line with GEMS policy
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Liaising with other IT teams in the network to raise and pre-empt potential online safety concerns
- Ensuring that any online safety incidents are logged, referred to the Designated Safeguarding Lead and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are referred to the Designated Safeguarding Lead dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

ICT Middle Leaders

Our Primary and Secondary Digital Leaders are responsible for:

- Ensuring all staff implementing the Computing curriculum, including links to STEAM are explicitly teaching students about online safety
- Quality assuring all levels of curriculum planning across the school to ensure there are explicit and implicit links to online safety education
- Raising awareness of integrating messages around online safety across all lessons where students use computers and electronic devices, including iPads and BYOD
- Supporting the safeguarding team with ongoing training for all staff, making use of the National Online Safety resources in addition to any other relevant training
- Ensuring there is ongoing awareness for parents, making use of the National Online Safety resources in addition to any other relevant training. This should include, but it not limited to, parental controls and advice around popular online platforms

- Liaising with other middle leaders in the network to raise and pre-empt any online safety issues

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the safeguarding team to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school anti-bullying policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the senior leadership team of any concerns or queries regarding this policy
- Ensure their child has read, understood , signed and returned the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- National Online Safety - National Online Safety
- What are the issues? – UK Safer Internet Centre
- Hot topics - Childnet International
- Parent resource sheet – Childnet International

The online resources above are intended for parent information only and is designed to fully inform parents of the risks that the internet may present to children and young people. Please note that UK sites may include content which is not in line with UAE cultural and Islamic values.

Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating Students about Online Safety

Students will be taught about online safety as part of the school curriculum:

In Key Stage 1, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of Primary School, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the end of Secondary School, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be promoted in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in emails or other communications home, and in information via our website and social media platforms. We will also run parent workshops to promote online safety during the academic year and give parents access to relevant National Online Safety training materials.

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and/or escalated in line with our Complaints Policy.

Concerns or queries about this policy can be raised with any member of staff, including senior leaders.

Cyber-bullying

Definition:

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of a person or group by another person or group, where the relationship involves an imbalance of power. (Also see the school Anti-bullying Policy.)

Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Moral Education, GroWell and any subjects where online platforms are used.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school supports parents about cyber-bullying strategies so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained, including cooperation with families and external agencies.

Confiscating Electronic Devices

The senior leadership team can confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Where unacceptable use of ICT is suspected, the senior leadership team will work with families and relevant external agencies, under the advice of the GEMS School Support Centre.

Any complaints about confiscating electronic devices will be dealt with through the school complaints procedure.

Acceptable Use of the Internet in School

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Students Using Mobile Devices in School

Primary students are encouraged to leave mobile devices at home. Where parents disagree with this, e.g. for safety reasons, mobile phones may be brought to school and stored in the child's bag. Bags are not stored in locked storage or inside the classroom. Sending mobile devices to school is at the parents own risk, and the school will not be held responsible for any loss or damage of mobile devices.

Secondary students may bring mobile devices into school, at their own risk. Secondary students may keep their mobile device in their bag or locker and are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Secondary Mobile Phones + Social Media

Students should not be using their mobile phones during the school day. If a student is using their phone, the following steps should be applied:

1. Teacher warns student – phone to go in bag or on teacher desk *(student agency)*
2. If seen again, the phone must go on the teacher's desk until the end of the day when the student should come back to collect it. This should be logged on Go4Schools.

Phones seen in the corridors should be given a warning. If more than once, teacher should keep on desk until the end of the day.

Social Media is not permitted to be used in school. Any students found to be using social media will have their device confiscated until the end of the school day.

Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT department.

How the School will Respond to Issues of Misuse

Where a student misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing or disrespectful messages
    - Sharing of indecent images and/or videos, especially around chat groups
    - Sharing of abusive images
- Most types of abuse can contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The Designated Safeguarding Lead and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every three years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Links with other policies

- Anti-bullying Policy
- Behaviour for Learning Policy
- Safeguarding Policy
- Whistleblowing Policy
- Feedback and Complaints Policy
- Staff Handbook

Appendix 1: KS1 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

When I use the school's ICT systems (like computers or school iPads) and/or the internet in school (e.g. using my own device) I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer/school iPad when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is illegal, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit on school systems and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and relevant visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or offensive material (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs or videos of students or staff on my own personal device
- Take photographs or videos of students on school devices without checking with teachers first
- Take photographs or videos of staff, parents or visitors on school devices without checking with the adults being photographed/recorded first
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school and permission has been granted by a senior leader

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT devices and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT team know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

أكاديمية جيمس ولينغتون - شارع الخيل
GEMS Wellington Academy
AL KHAIL

WEK Bring Your Own Device Acceptable Use Policy
Key Stage 2

This document covers the use of BYOD technologies in the school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems. Digital systems, technologies and software are made available to students to further their education and to help the management of the school. This Acceptable Use Policy has been drawn up to protect students, staff and the school. The school reserves the right to examine or delete files that may be held on its computer systems and to monitor any Internet site visited or work done by a user.

- I understand that I must use the school digital system in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the digital systems and other users.

For my own personal safety:

- I understand that only tablets and laptops suitable for learning will be used in school. No mobile phones without exception.
- I understand that the school will monitor my use of the digital systems. Teaching staff will only be able to **read** information in My Documents and not amend anything.
- I understand that the school digital systems are for educational use only. I will only use devices for school work, homework and as directed.
- I will not bring files into the school without permission or upload inappropriate material to my workspace.
- I will only edit or delete my own files and not view, or change, other people's files without their permission.
- I will keep my logins, usernames and passwords secret. I will not share it, nor will I try to use any other person's username and password.
- I will make sure there are no social media applications on my device while in school
- I will use the Internet responsibly and will not visit web sites I know to be appropriate for the school.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a teacher / trusted adult.
- I will not share personal information about myself or others when on-line.

- I will never arrange to meet someone I do not know on the internet.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use VPNs or use other private networks while using devices at school.
- I understand that I am responsible for my actions, both in and out of the school.
- I understand that the School also has the right to act against me if I am involved in inappropriate behaviour that are covered in this agreement.
- I understand that if I break any rules in this Acceptable Use Policy Agreement, I will face consequences. This may include removal of devices, contact with parents and in the event of illegal activities involvement of the appropriate authorities.

User Signature – Acceptance of the above conditions:

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the School's most recent digital-safety policies.

Student Name: ______________________________________ Class:
____

Signature: ______________________________________

Parent Name: ______________________________________

Signature: ______________________________________ Date: