: Learners Today.. Leaders Tomorrow :

The Gulf English School

Online Safety Policy

Date: October 2026

Author: E-Learning Manager/LT

Adoption / Review	Committee	Lead Personnel	Review Date:
October 2026	LT/IT/E-learning	E-Learning Manager	October 2027

This policy applies across all campuses:
GES Gharafa (Infants, Juniors, and Secondary),GES Bin Omran

Responsible, **R**espectful, **R**esilience

Our Vision

We aim to develop a responsible, respectful, resilient school community, supporting the highest level of personal achievement in a changing modern intercultural world.

V1	We aim to develop a responsible, respectful, resilient school community,
V2	supporting the highest level of personal achievement
V3	in a changing modern intercultural world.

Mission Statements

M1	We provide a high-quality education, focusing on skills, knowledge and application, enabling our community to strive and achieve excellence
M2	We aim to develop a culture of life-long learning, independence, ambition, which is continuously demonstrated by our community.
M3	Our community promotes diversity and global citizenship where individual differences are understood and celebrated.
M4	To drive the development of creative skills and critical awareness in our students.
M5	Our school community provides a safe, supportive, and stimulating learning environment that focusses on the well-being of all
M6	We aim to integrate the use of technology on a day-to-day basis to enhance our teaching and learning.

Our Core Values: The 3 R's

- ✓ **Responsible:** Driven, Ambitious, Achiever
- ✓ **Respectful:** Empathy, supportive, caring, diversity
- ✓ **Resilient:** Risk takers, empowered, committed

Key People

The Gulf English School	**Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring**	Heads of School: Bin Omran, Infants, Juniors and Secondary
	Deputy Designated Safeguarding Leads / DSL Team Members	Deputies of Schools
	Curriculum leads with relevance to online safeguarding and their role	E-Learning Manager, Director of Studies
	Network manager / other technical support	IT Network Manager (day-to-day management of filtering and monitoring systems)
	Date this policy was reviewed and by whom	October 2026 by E-Learning Manager
	Date of next review and by whom	October 2027 by E-Learning Manager (earlier review when the AI Policy is adopted)

Regulatory Context

This policy takes account of applicable Qatar legislation and Ministry of Education and Higher Education (MOEHE) requirements, including student protection and safeguarding guidance for private schools, Qatar Law No. 13 of 2016 concerning Personal Data Privacy Protection, and relevant cybercrime legislation.

It is also informed by UK Department for Education guidance, including *Keeping Children Safe in Education (2026)*, *Teaching Online Safety in Schools*, filtering and monitoring standards, and guidance on generative AI in education.

UK guidance is applied as a benchmark for good practice, subject to Qatar legislation and MOEHE requirements. The school will review relevant regulatory updates and amend its procedures where necessary.

Related GES Policies and Procedures

This policy should be read alongside the GES Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Admissions Policy, SEND/Inclusion and EAL arrangements, PSHE and Curriculum Policies, BYOD Policy, Acceptable Use Agreements, Data Protection and Image Consent arrangements, Staff Code of Conduct, Staff Handbook, Complaints Policy and Educational Visits Policy.

Where online incidents involve bullying, inappropriate behaviour or potential harm to a pupil, safeguarding procedures take priority. Any subsequent behavioural or disciplinary action must be coordinated with the DSL and relevant Head of School.

What is this policy?

Online safety is an integral part of safeguarding at The Gulf English School (GES). This policy establishes a whole-school approach to protecting pupils, staff and the wider school community when using digital technology, both within and beyond the school environment.

It outlines expectations for safe and responsible technology use, online safety education, filtering and monitoring, and the procedures for identifying, reporting and responding to online risks, including cyberbullying, harmful content, online abuse and emerging technologies such as artificial intelligence (AI). All online safeguarding concerns must be managed in accordance with the GES Safeguarding and Child Protection Policy, with the Designated Safeguarding Lead (DSL) overseeing the appropriate response.

Policy Aims:

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all The Gulf English School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Developing students' digital citizenship: the knowledge, skills and values to use technology safely, responsibly, respectfully and critically, in line with our core values (the 3 R's).
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope:

This policy applies to all members of The Gulf English School community (including teaching, supply and support staff, governors, volunteers, contractors, students/students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role. It covers school-owned devices and

personal devices (including mobile phones, smartwatches, tablets and laptops) used on site, on school trips and in school-related activities, as well as online behaviour outside school that affects members of the school community.

The 4 C's – Understanding online risks

Following KCSIE, staff use the four Cs to identify, discuss and record online safety concerns. The risks in each area change quickly, so staff and students are updated regularly, including on risks linked to AI.

- **Content:** being exposed to illegal, inappropriate or harmful material, such as pornography, extreme violence, racism, misogyny, antisemitism, radicalisation and extremism, self-harm, suicide and eating disorder content, and misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** harmful interaction with others online, including grooming, sexual or criminal exploitation, harassment, contact from strangers on social media and gaming platforms, and interaction with AI chatbots and companion apps that simulate human relationships.
- **Conduct:** online behaviour that increases risk or causes harm, including cyberbullying, making, sending or receiving nude or semi-nude images (including images created or altered using AI, such as deepfakes), sharing others' private information or images, and misusing AI tools to harass, humiliate or deceive others.
- **Commerce:** online gambling, inappropriate advertising, phishing, scams, and pressure to spend money in games and apps.

Roles and Responsibilities: Accountability and oversight

The Heads of School act as campus DSLs and have operational safeguarding responsibility. The cross-campus Deputy DSL provides cover and advice. The IT Network Manager is the technical lead for filtering, monitoring, access controls and cyber-security; the E-Learning Manager supports curriculum implementation and digital-safety education; the Director of Studies supports curriculum coordination. The General Manager and Board provide strategic oversight and receive an appropriately anonymised annual online-safety assurance report. Technical management does not transfer safeguarding decision-making from the DSL.

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in the Appendix – Roles at the end of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also student, governor, etc. role descriptions in the appendix. All staff have a key role to play in feeding back on potential issues

Education and Curriculum

Inclusive and age-appropriate provision

Online safety education is sequenced across EYFS, primary and secondary phases through Computing, PSHE/form time, assemblies and relevant subjects. Teachers adapt content, vocabulary, communication methods and reporting routes for pupils with SEND, EAL needs or additional vulnerabilities, including those with limited digital literacy or who may be disproportionately targeted online. The Learning Support/EAL teams and DSL advise on reasonable adjustments, targeted interventions and individual online-safety risk assessments where appropriate. Online safety learning is accessible to pupils admitted mid-year through induction and catch-up support.

Despite the risks associated with being online, The Gulf English School recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what students have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help students navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of students, including vulnerable students.

The teaching of online safety, features in these particular areas of curriculum delivery:

- Computing
- Citizenship
- Assemblies, awareness sessions and whole-school campaigns

However, as stated previously, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Digital Citizenship

Digital citizenship is the ability to use technology safely, responsibly, respectfully and critically. At GES we link it directly to our core values:

- **Responsible:** using devices and AI tools honestly and for learning, protecting personal information, respecting copyright and academic integrity, and managing screen time and sleep.
- **Respectful:** treating others online as we would face to face, asking permission before filming, photographing or sharing others, and challenging and reporting bullying or hateful behaviour.
- **Resilient:** recognising scams, manipulation, misinformation and pressure online, knowing how and where to get help, and supporting friends who are struggling.

Digital citizenship and online safety are taught progressively from the Infants to the Sixth Form, informed by the UKCIS framework Education for a Connected World, and include the safe and critical use of AI tools.

Working with Staff and Parents

Online safety is a shared responsibility between school and home. We will:

- provide online safety and filtering and monitoring training for all staff at induction and annually, with updates when new risks emerge (including AI-related risks);
- provide regular guidance and awareness opportunities for parents/carers, for example information sessions, newsletters and resources on social media, gaming, device boundaries at home and AI;
- involve students and parents in reviewing how well our approach works, so that the policy reflects real practice.

Handling Safeguarding concerns and incidents

Recording, response and local escalation

Any immediate risk of harm must be brought directly to the campus DSL or available Deputy DSL without delay, with the concern recorded promptly using the GES safeguarding referral system. Staff must not investigate independently, promise confidentiality, confront alleged perpetrators or circulate harmful material. The DSL records the risk assessment, protective actions, parent-contact decision, referral rationale, follow-up and closure. Where concerns involve criminal conduct, exploitation or immediate danger, the DSL/Head of School follows the GES Safeguarding and Child Protection Policy and applicable Qatar Police and MOEHE Student Protection and Care Officer reporting pathways. Information is shared only with those who need it for safeguarding, with secure records and appropriate retention.

Safeguarding, behaviour and anti-bullying interface

Cyberbullying, discriminatory abuse, impersonation, harmful group chats, threats and non-consensual sharing of images are considered under the Anti-Bullying and Behaviour Policies, but the DSL first determines whether they are child-on-child abuse or another safeguarding concern. The school will support the affected pupil, assess risks to other pupils, consider proportionate educational and disciplinary responses, monitor recurrence and communicate with parents when safe and appropriate.

Conduct outside school is addressed where it affects pupil welfare, safety or the school community. Any complaint about the school's handling is managed under the Complaints Policy without replacing safeguarding reporting.

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Bring Your Own Device (BYOD) Policy, including the mobile phone rules
- Staff Code of Conduct

This school commits to take all reasonable precautions to safeguard students online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on the form found on the Intranet- this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

If the DSL or a deputy is not available, staff must report to another member of the safeguarding team or a senior leader straight away. A concern must never wait because one person is unavailable.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

The following sub-sections provide detail on managing particular types of concern.

Safeguarding response: mandatory steps for all online incidents, including cyberbullying

The Safeguarding and Child Protection Policy is the controlling procedure for all online safety concerns, including cyberbullying, online harassment, threats, coercion, exploitation, discriminatory abuse, image-sharing, impersonation, harmful AI-generated content and incidents arising outside school that affect pupils. Staff must not treat a potential safeguarding concern solely as a behaviour issue or conduct their own investigation.

1. Recognise and respond: listen calmly, take the pupil seriously, reassure without promising confidentiality, avoid blame or leading questions, establish whether there is an immediate risk and take proportionate steps to protect the pupil. Where there is immediate danger, seek emergency assistance through the appropriate Qatar emergency services and notify the DSL without delay.

2. Report promptly: inform the campus Designated Safeguarding Lead (Head of School) immediately for urgent concerns and otherwise as soon as possible on the same day. Use the school intranet safeguarding referral form to record the concern; an electronic submission does not replace speaking directly to the DSL in urgent cases. If the DSL is unavailable, contact the cross-campus Deputy DSL (Director of Studies) or another Head of School/DSL; escalate to the General Manager when necessary. Never defer action because a named colleague is absent.

3. Make a factual record: record the pupil's words where possible, dates, times, individuals involved, relevant platforms, the nature and impact of the concern, action taken and to whom it was referred. Use the school's secure safeguarding system and restrict access on a need-to-know basis. Do not circulate allegations or sensitive pupil information through ordinary group chats or personal accounts.

4. Preserve evidence safely: do not ask pupils to forward harmful material or take additional screenshots. Record usernames, URLs and contextual details only where safe and appropriate. Do not view, download, copy, print, forward or delete nude or semi-nude images of children; leave any device handling and evidential decisions to the DSL and relevant authorities. The IT Network Manager may preserve technical logs only under DSL direction and approved procedures.

5. Assess and protect: the DSL undertakes and records a safeguarding risk assessment, considering the child's wishes and safety, power imbalance, repetition, vulnerability (including SEND/EAL), discriminatory elements, potential criminality, risk to other pupils and whether the matter requires immediate protection, supervision, separation or adjustments. Online bullying is addressed under the Anti-Bullying Policy and any associated pupil misconduct under the Behaviour Policy, without replacing the safeguarding response.

6. Decide on referrals and notifications: the DSL follows the Safeguarding and Child Protection Policy and applicable MOEHE Student Protection and Care reporting routes, including referral to the appropriate Qatar authorities or police where required. Inform parents/carers as appropriate, unless doing so could increase risk to a child or compromise a statutory response. The Head of School and General Manager are informed in line with the school's escalation arrangements.

7. Support all pupils: agree a proportionate safety and pastoral support plan for the pupil affected and, where appropriate, other pupils involved; consider supervision, trusted adult contact, counselling,

SEND/EAL support, safe use of platforms and restorative measures only where suitable and not harmful. Avoid automatic mediation in cases involving coercion, exploitation or serious power imbalance.

8. Investigate behaviour separately and fairly: where appropriate, the Head of School coordinates a proportionate fact-finding process under the Behaviour and Anti-Bullying Policies, keeping safeguarding records and disciplinary decisions appropriately separated. Apply consistent, age-appropriate sanctions and educational interventions, while safeguarding all children involved. Serious staff-related allegations must follow the staff allegations and safer-working-practice procedures.

9. Monitor, review and close: the DSL records actions, referrals, parent communication, pupil voice, follow-up dates and outcomes; checks that harm has stopped and there is no retaliation; reviews any ongoing risks; and escalates unresolved or repeated incidents. Close the case only in accordance with safeguarding recordkeeping and retention procedures. The safeguarding team reviews patterns and trends across campuses, including cyberbullying and repeated platform misuse, and informs leadership action.

10. Confidentiality and information sharing: share information promptly when necessary to protect a child, using authorised secure systems and relevant Qatar data protection requirements. Staff must not promise secrecy, conduct informal digital searches or independently contact alleged perpetrators or their families before the DSL has assessed the risk.

Pupil and Parent Reporting

Pupils and parents may report cyberbullying and online concerns to a class teacher/form tutor, Head of School/DSL, or the school's established safeguarding referral routes. Where available to the relevant campus, the Speak Up reporting channel on Microsoft Teams provides an additional route; it does not replace urgent direct reporting. Staff receiving a report must follow the same safeguarding steps above, even when the incident occurred outside school hours.

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Online child-on-child abuse, and nude and semi-nude images

Online child-on-child abuse includes cyberbullying, online sexual harassment, pressuring or coercing others to share images, sharing private messages or images, and abusive group chats or gaming interactions. It is never dismissed as 'banter' or 'just online'. Incidents often start outside school and then affect students in school; they are handled under the Safeguarding and Child Protection Policy.

Making, sending or sharing nude or semi-nude images of anyone under 18 is a serious safeguarding matter and may be illegal. This applies even when the image was shared willingly, and it includes images created or altered using AI (for example deepfakes and 'undressing' apps). Every incident requires a safeguarding response. If a student discloses an incident, or staff become aware of one, staff must:

- stay calm, reassure the student and avoid victim-blaming language;
- **not** view, copy, print, screenshot, forward or delete any image, and ask the student not to forward or delete anything either;
- secure any device involved and report to the DSL or a deputy immediately, on the same day (see Searching and confiscation);
- leave decisions about next steps to the DSL, who will assess risk, support everyone involved, inform parents/carers unless this would put a child at risk, and make onward referrals (including to the Police or other agencies) where required.

Other online safeguarding concerns

Staff should be alert to the following, and report any concern to the DSL:

- grooming, sexual or criminal exploitation, and sextortion (blackmail using intimate images);
- radicalisation and extremism online, including extreme misogyny and harmful online influencers;
- exposure to harmful content, including self-harm, suicide, eating disorder, pornographic and extreme violence content;
- contact with strangers through social media, messaging apps, livestreams and gaming chat;
- unhealthy reliance on AI chatbots or companion apps for emotional support or advice;
- scams, gambling and financial pressure online; and
- changes in a student's behaviour, mood, sleep or friendships, or secrecy around devices, which may signal that something is wrong online.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where students contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.
It will be necessary to reinforce these as usual at the beginning of any school year but also to remind students that **the same applies for any home learning** that may take place.
Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Appropriate filtering and monitoring

Annual assurance and testing record

The IT Network Manager and campus DSLs will maintain a documented filtering and monitoring review at least annually and following material changes to systems, risk or pupil use. The review will identify system coverage and limitations; age-appropriate filtering groups; school-managed and BYOD access; safeguarding alert thresholds; named alert recipients and cover arrangements; response times; testing on representative devices and accounts; overblocking and bypass attempts; AI-related risks; and actions, owners and deadlines. The senior leader overseeing the review will report key risks and completion of remedial actions to the General Manager/Board. Staff remain responsible for active supervision: technical filtering alone is not sufficient.

Cybersecurity and incident coordination

The IT Network Manager will maintain proportionate security controls, including managed access rights, prompt account removal for leavers, software and security updates, malware protection, secure backups, multi-factor authentication where supported, and a documented response to suspected compromise. A cyber incident involving pupil welfare must be referred to the DSL; suspected loss, disclosure or misuse of personal data must also be escalated promptly to the designated data-protection lead for assessment under Qatar requirements. Any external notification is determined by the authorised school lead, not by individual staff.

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place. The IT Network Manager manages the filtering and monitoring systems day to day. This is in line with the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

In practice

- The IT Network Manager manages, maintains and tests the filtering and monitoring systems; checks that they work on school devices and on the school Wi-Fi, including personal (BYOD) devices; keeps a record of changes and checks; and reports any alert or concern to the DSL immediately.
- The DSL and safeguarding team review alerts and reports, decide what action is needed, record concerns in the same way as any other safeguarding concern, and ensure staff understand their role.
- The senior leader responsible leads a documented review of filtering and monitoring at least once a year, and again when a new risk, system or technology is introduced. The review checks that systems are working, what is blocked and allowed for whom, and how well alerts are handled, and records actions taken.
- Filtering and monitoring must also take account of generative AI tools and AI-generated content.

- All staff report overblocking, gaps in protection and any attempt by students to bypass the systems. Students are taught to report harmful content that gets through.

Limits of filtering and monitoring. Our systems protect the school network and school-managed devices. They cannot control a personal phone using mobile data (4G/5G), a personal hotspot or a VPN. This is one of the main reasons students hand in their phones during the school day and why VPNs, hotspots and other external connections are not allowed on our network (see the BYOD Policy).
The school's filtering and monitoring systems are **Content Keeper**

Annual filtering and monitoring assurance report

The IT Network Manager will prepare and provide a documented filtering and monitoring report, and following significant changes or incidents, to the relevant Heads of School/DSLs, General Manager and governing Board through the agreed safeguarding oversight arrangements. The IT Network Manager is responsible for technical evidence and recommendations; the DSLs retain responsibility for evaluating safeguarding implications and following up concerns.

The report should record the filtering and monitoring products and coverage (including Content Keeper), testing dates and results, protection on school-managed devices and school Wi-Fi, known limitations for mobile data/hotspots/VPNs, blocked and permitted categories, monitoring alert processes, significant incidents or bypass attempts, actions taken, unresolved risks, named owners and completion dates. It should also assess access for different age groups and vulnerable pupils and confirm that necessary educational content is not unreasonably blocked.

The IT Network Manager should maintain a technical change and testing log and notify the DSL immediately of any serious gap or safeguarding alert. The E-Learning Manager supports curriculum impact and staff training. Heads of School/DSLs review the report, record safeguarding decisions and corrective actions, and ensure the annual review is reported to the Board. Where a control is not yet in place, this must be recorded transparently with interim mitigation and an implementation deadline; the report is evidence of review, not proof that every technical risk has been eliminated.

Cross-policy consistency, induction and admissions

This policy is read with the Safeguarding and Child Protection, Anti-Bullying, Behaviour, SEND/Inclusion, EAL, BYOD, Acceptable Use, Data Protection, Staff Code of Conduct, Admissions, Home–School Agreement and relevant School Handbooks. At admission and induction, pupils and parents receive age-appropriate expectations for safe use of school systems, reporting cyberbullying, personal devices, consent for images and respectful online behaviour. The Admissions Team shares relevant safeguarding and learning-support information securely with the receiving Head of School/DSL and inclusion staff on a need-to-know basis, in accordance with the Admissions and Safeguarding Policies.

Staff induction and annual refreshers cover reporting pathways, child-on-child abuse, cyberbullying, online image incidents, filtering and monitoring responsibilities, safe communications, AI-related risks and secure data handling. The school records participation and follows up outstanding acknowledgements.

Online safety education and reporting routes are adapted where necessary for pupils with SEND, EAL or other vulnerabilities.

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised Systems

- Students at this school communicate with each other and with staff using Office 365 Email and Microsoft Teams
- Staff at this school use the email system provided by Office 365 for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.
- Staff at this school use SchoolBase, Class Dojo and Class Charts to communicate with parents.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.
Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head of School (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Head of School/GM (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles of messaging/commenting systems

- More detail for all the points below are given in the section of this policy as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Students and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Use of generative AI and emerging risks

AI approval, privacy and academic integrity

GES is currently reviewing and developing its approach to the safe and responsible use of artificial intelligence (AI) across the school.
Staff may use school-approved AI tools, including Microsoft Copilot and Claude, where appropriate for educational and professional purposes. However, identifiable pupil information, safeguarding records, medical details, assessment data and confidential school information must not be entered into public or unapproved AI systems.

Pupil use of AI must be age-appropriate, supervised by staff and consistent with platform age restrictions and school expectations.
These arrangements remain a work in progress and will be reviewed and refined as the school develops its formal AI Policy, taking account of safeguarding, data protection and emerging guidance.

AI-generated content must be checked for accuracy, bias and suitability; any AI-assisted work must comply with assessment and academic-integrity expectations. AI-generated bullying, impersonation, fabricated intimate imagery and harmful chatbot interactions must be reported immediately to the DSL.
This section will be reviewed when the separate GES AI Policy is adopted.

Generative AI tools (such as ChatGPT, Microsoft Copilot, Google Gemini, Claude, image and video generators, voice-cloning tools, and AI features built into search engines, social media and apps) are now part of everyday life for students, staff and families. They offer real benefits for learning, creativity and workload, and they carry real risks. KCSIE 2026 and DfE guidance expect schools to address AI within online safety, filtering and monitoring, the curriculum and staff training. We follow the DfE's guidance on generative AI in education.

Our current position. The school does not currently place a blanket restriction on the use of AI tools by students or staff. Instead, we rely on the principles below, on teachers' instructions for specific tasks, and on the Behaviour Policy and Acceptable Use Agreements. A dedicated AI Policy is being developed and will be in place by the end of this academic year, together with training for staff. This section will be reviewed when that policy is approved.

Principles that apply now

- **Honesty.** Teachers will tell students when and how AI may be used for a task; if students are unsure, they must ask. Students must not present AI-generated work as their own where this is not permitted. The use of generative AI in exams and formal assessments, or to plagiarise and cheat, is prohibited unless explicitly allowed, and the Behaviour Policy will be used for any student found doing so.
- **Privacy.** Personal information about students or staff (names, photographs, assessment data, safeguarding or special educational needs information) must not be entered into public AI tools. Staff must not upload identifiable student data into AI tools that the school has not approved.
- **Respect and safety.** AI must never be used to create, alter or share images, audio, video or text that imitate, humiliate, harass, deceive or sexualise another person (for example deepfakes, voice

cloning and 'undressing' apps). This is treated as serious misconduct and a safeguarding matter, and may involve the Police.

- **Critical thinking.** AI can be wrong, biased or make things up. Students and staff are expected to check outputs and sources, and students are taught to question what they see and read online.
- **Wellbeing.** AI chatbots and companion apps can feel like friends and can give harmful or inaccurate advice. Students are encouraged to talk to a trusted adult about anything that worries them, and staff who notice a student relying on a chatbot for emotional support should speak to the DSL.
- **Age limits.** Many AI tools have minimum ages, typically 13 or older or 18 with parental consent. Parents are encouraged to check the terms of the tools their children use.
- **Staff use.** Staff may use AI to support planning and administration, but remain responsible for accuracy, safeguarding and data protection. AI must not replace professional judgement in safeguarding, assessment or behaviour decisions.
- **Tools used in lessons.** Where teachers direct students to use an AI tool as part of a lesson, the tool should first be checked for age suitability, data protection and filtering and monitoring.

We will keep talking about AI with students, staff and parents, covering both its practical use and its ethical pros and cons. We know many students use AI at home and may meet both positive and negative experiences there, including inappropriate use of data, misinformation, bullying, deepfakes and 'undressing' apps. Training for staff on AI-related risks will be delivered alongside the AI Policy.

School website

Publication and image consent

Pupil photographs, videos, names, work and other identifying information may be published only in accordance with current parental consent, pupil welfare considerations and the school's Data Protection and photography/image-use arrangements. Staff must check consent status before posting and remove content promptly where consent is withdrawn or a safeguarding concern is identified. School communication channels and accounts must remain centrally controlled.

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head of School and the leadership team have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the IT Network Manager.

Social media

Social Media presence

The Gulf English School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and inspectors may also look at what is being said online.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, students' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

As outlined in the Acceptable Use Policies, students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head of School and should be declared upon entry of the student or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head of School (if by a staff member).

Students should also understand that screenshots, group chats, 'disappearing' messages and anonymous accounts are not private or free from consequences. Anything shared online can be copied and forwarded. Where online behaviour affects members of the school community, it will be dealt with under the

Behaviour Policy and, where needed, the safeguarding procedures, whether it happens in or outside school.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

Inappropriate use of social media or technology by staff can lead to disciplinary action, referral to professional regulatory bodies and, in serious cases, police involvement.

All members of the school community are reminded that, particularly in the context of social media, it is important to comply with the school's Data Protection Policy and image consent arrangements, and that permission must be sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with students or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, digital images and video, and the BYOD Policy.

Use of school devices

Staff and students are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.
School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.
Wi-Fi is accessible to students, guests and teacher for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
Personal devices (BYOD) may connect to the school student Wi-Fi only, as set out in the BYOD Policy. Personal hotspots, mobile data used to access the internet during lessons, VPNs and anonymising services are not permitted on site.
School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use. All and any usage of devices and/or systems and platforms may be tracked.

Mobile phones, smartwatches and personal devices

Consistency with BYOD and individual safeguards

The detailed restrictions, hand-in arrangements and any Sixth Form exceptions remain governed by the GES BYOD Policy and Behaviour Policy. Any agreed medical, SEND or safeguarding exception must be individually risk-assessed, approved by the relevant Head of School with DSL input and communicated discreetly to staff who need to know. Personal devices must not be used to bypass school filtering through mobile data, hotspots or VPNs. Searches of devices or suspected intimate imagery must be referred to the DSL and managed lawfully and sensitively; staff must not routinely search private content or view/copy indecent images.

GES is a mobile-phone-free school for students during the school day, in line with current DfE guidance that schools should be mobile-phone-free by default (KCSIE 2026). This protects learning and wellbeing and reduces safeguarding risk: personal phones give unfiltered mobile data access, can bypass school filtering and monitoring, and are a common route for cyberbullying, image-sharing and contact with strangers. The full procedures are in the Mobile Phone Policy section of the BYOD Policy. In summary:

Students

- Students may bring a mobile phone to school, at their own risk, but must hand it to their form tutor at the start of the day. It is returned at the end of the school day.
- Students who arrive late sign in at Reception, collect a late slip and hand their phone in at Reception.
- Sixth Form students may keep their phone on their person but may use it only in the Boys'/Girls' Majlis area and nowhere else on campus.
- Smartwatches, earbuds and any other device that can send or receive messages, access the internet, take photographs or record are treated in the same way as a mobile phone, unless an exception has been agreed.
- Parents who need to reach their child during the school day should contact Reception rather than calling or messaging the student. Students who are unwell or involved in an incident should report to a member of staff first, not contact home directly.
- No student may photograph, film or record other students or staff without permission, on any device.
- Exceptions (for example medical needs or SEND support) are agreed in advance with the Head of School and recorded.
- A student found using, or in possession of, a phone outside these arrangements will have it confiscated, and the sanctions in the BYOD and Behaviour Policies will apply. Parents will be informed. If there is any safeguarding concern about how a device has been used, the DSL is informed immediately.

Staff

- Staff model the expected behaviour. Personal phones are kept out of sight and on silent when teaching or supervising students, and used in staff areas, except for emergencies or approved school purposes (for example multi-factor authentication).
- Staff never use personal phones, personal email, WhatsApp or social media accounts to contact students or parents. Only the authorised systems listed in this policy are used.
- Staff do not take photographs or video of students on personal devices. School-owned devices or approved school accounts are used, and images are kept only on school systems.
- Staff who access school email, Teams or other school data on a personal device must protect it with a passcode or biometric lock, keep it updated, and report loss or theft to IT immediately.

Parents, visitors and contractors must not use phones or other devices to photograph or record students on site (see social media), and should follow any instructions given on arrival.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Head of School and staff authorised by them have a statutory power to search students/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Searches of a device are carried out only by staff authorised by the Head of School, with a second adult present wherever possible. Staff must not view, copy or forward suspected nude or semi-nude images of a child; they secure the device and pass it to the DSL, who decides the next steps. Parents are informed of any search or confiscation.

Appendix – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "All Staff" section as well as any other relevant to specialist roles.

Roles:

- All Staff
- Head of School
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Students
- Parents/carers

Parent partnership and concerns

Parents and carers should report cyberbullying, unwanted contact, harmful content, impersonation or misuse of a pupil's images promptly to the school, including incidents originating outside school that affect pupils. The school will provide practical guidance on privacy settings, age ratings, scams, gaming, AI tools and reporting concerns, and will explain the school's safeguarding and complaints routes. Information will be shared sensitively, taking account of the safety and privacy of all children involved.

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the designated safeguarding lead as named in the AUP, maintaining an awareness of current online safety issues (see 'Understanding online risk: the

four Cs' and 'Use of generative AI and emerging risks') and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or students bypassing protections. All staff are also responsible for the physical monitoring of students' online devices during any session/class they are working within.

All staff, including those who do not work directly with children, must read Part 1 of KCSIE (2026). All staff must also understand the mobile phone and personal device rules in this policy, the risks linked to AI-generated content, and how to report a concern to the DSL.

Head of School

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements (National College Platform)
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for students in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised.
- Ensure the mobile phone arrangements are applied consistently by all staff, communicated clearly to students and parents, and reviewed regularly.

- Oversee the development and approval of the school's AI Policy and the related staff training.
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead – Heads of School

Key responsibilities (remember the DSL can delegate certain online safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to students confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training via National College Platform (including online safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles.
    - All staff must read KCSIE Part 1 in full (the condensed Annex A for staff who do not work directly with children has been withdrawn in KCSIE 2026), and those working with children should also read the further information in Annex A (formerly Annex B).
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the Head of School, DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection
- n is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the the governing body / school leadership.
- Receive regular updates about online safety issues and legislation, be aware of local and school trends

- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for students to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Make sure DSL cover is always available, so that staff can report a concern at any time (for example through a monitored shared safeguarding mailbox), and that staff know what to do if the DSL and deputies are unavailable.
- Make sure response procedures cover AI-generated images (deepfakes), AI chatbot concerns and mobile phone incidents, and that staff are trained to follow them.

Governing body and school leadership oversight

Key responsibilities:

- Receive at least an annual report on online safety, including trends in incidents (anonymised), the outcome of the filtering and monitoring review and the effectiveness of the mobile phone arrangements.
- Make sure the DSL, the senior leader responsible for filtering and monitoring, and the IT Network Manager have the time, training and resources they need.
- Ask questions of leaders about online safety, AI and mobile phone practice, and challenge where needed.

Computing Lead – E-Learning Manager

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the PSHE curriculum, and model positive attitudes and approaches to staff and students alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.

- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online safety element.

Network Manager/other technical support roles

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks
- Manage the day-to-day operation of filtering and monitoring on the school network and school-managed devices, including personal devices connected to the school Wi-Fi; carry out and record regular checks; support the annual review led by the senior leader and DSL; and report alerts or concerns to the DSL immediately.
- Block or restrict VPNs, proxies, anonymising services and unauthorised hotspots on the school network as far as is technically possible, and make sure filtering and monitoring take account of generative AI tools.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Work with the Head of School to ensure the school website meets statutory DfE requirements.

The **IT Network Manager currently undertakes the role of Data Protection Officer (DPO)** at The Gulf English School, overseeing data protection and information security arrangements across all campuses.

Key Responsibilities:

- Provide guidance, training and support to staff on data protection, cybersecurity and the secure handling of personal information, ensuring consistency with relevant GES policies and applicable Qatar legislation.
- Ensure that data protection procedures do not unnecessarily restrict the sharing of information required to safeguard and protect pupils. Information must be shared appropriately, securely and on a need-to-know basis in accordance with the Safeguarding and Child Protection Policy.

- Oversee the secure storage, retention and disposal of pupil and safeguarding records, in consultation with the relevant Designated Safeguarding Lead (DSL), and in accordance with applicable MOEHE requirements and Qatar data protection legislation.
- Ensure access to confidential pupil and safeguarding information is restricted to authorised personnel, with appropriate monitoring, access controls and audit procedures.
- Work closely with the Heads of School, DSLs and school leadership to identify and address data protection risks, including those associated with online platforms, artificial intelligence and emerging technologies.
- Review data protection and cybersecurity arrangements regularly and recommend improvements where necessary.

The DPO role and associated procedures will remain under review as the school continues to develop and strengthen its data protection and information security arrangements.

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a student. The same applies to any private/direct communication with a student.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use agreement and the BYOD Policy.
- Follow the mobile phone rules: phones are handed in at the start of the day (or at Reception if late), and Sixth Form students use phones only in the Majlis area.
- Use technology and AI tools honestly and responsibly, and follow teachers' instructions on when and how AI may be used.
- Treat others online as they would face to face; never use devices or AI to bully, record, impersonate or humiliate others, or to create or share harmful images.
- Tell a trusted adult straight away about anything online that worries or upsets them, or someone else. They will be supported, not blamed.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the student AUP and encourage their children to follow it.
- Support the school's mobile phone rules: contact your child through Reception during the school day rather than by phone or message, and talk to your child about why the rules exist.
- Talk regularly with your child about the apps, games and AI tools they use, who they talk to, and how long they spend online. Agree clear limits, including keeping devices out of bedrooms

overnight. School filtering does not cover your child's phone, mobile data or home internet, so consider parental controls at home.
- Respect the minimum age limits of social media, games and AI tools.
- Do not film, photograph or share images of other people's children, and do not post negative comments about the school, staff or other families online. Raise any concerns with the school directly.
- Report any online safety concern involving your child, or another child, to the school.

External groups

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers.

Policy Implementation, Monitoring and Review

The Gulf English School is committed to providing a safe and secure digital environment for all members of its school community. This policy establishes the school's expectations and procedures for online safety and will be implemented alongside the GES Safeguarding and Child Protection Policy and other relevant school policies.

Online safety is a shared responsibility, with the Heads of School, Designated Safeguarding Leads, IT Network Manager and wider school community contributing to its effective implementation.
This policy is a working document and will be reviewed annually, or sooner where necessary, to reflect emerging online risks, technological developments, changes in school practice and applicable MOEHE requirements.

Any amendments will be subject to review and approval through the school's established leadership and governance procedures.