

	Integrated Management System	Document ID	AD3/EA
		Revision No.	1
		Issue Date	10-Jun -2024
	Quality Procedures for IT, Digital Technology and Online Safety Policy		

Integrated Management System (IMS)
IT, Digital Technology and Online Safety Policy



This Document has been reviewed and approved by:

Name	Position	Signature
Hiba Khateeb	QMR	<i>Hiba</i>
Michael Hughes	Principal	
Samia Mughrabi	CEO	

Revision History of the Document

Revision No.	Issue Date	Summary of Changes	Responsibility	References
1.0	13-May -2026	Initial Edition	IT Lead	

This document has been approved by the School Management System

The only approved and controlled copy of this document is the one available electronically on the school's network. Printing and distributing of this document are prohibited. Users must verify the Revision Number and Issue Date of the document before use.

Page 1 of 28

IT, Digital Technology and Online Safety Policy

Content

- 1- Rationale**
- 2- Purpose**
- 3- Scope**
- 4- Policy Principles and British Values**
- 5- Acceptable Use of IT Systems**
- 6- Online Safety and Digital Citizenship**
- 7- Learner use of Mobile Phones, Cameras and Handheld Devices**
- 8- Staff use of Mobile Phones, Cameras and Handheld Devices**
- 9- Online Safety Sanctions**
- 10- Cyber Security and Data Protection**
- 11- Roles and Responsibilities**
- 12- Staff training and Learner Education**
- 13- Monitoring, Recording and Quality Assurance**
- 14- Terms and definitions**
- 15- Procedures**
- 16- Related forms and documents.**

1. Rationale

New Dawn Private School recognises that information technology and digital technologies are essential to high-quality teaching, learning, assessment, communication, administration and school operations. When used effectively, technology supports innovation, creativity, collaboration, digital literacy and the development of the knowledge and skills learners need to succeed in a changing world.

The school is committed to ensuring that all technology is used safely, ethically, responsibly and in a manner that protects learners, staff, visitors, school information and the wider school community. This includes preventing and responding to online harm, cyberbullying, inappropriate content, unauthorised photography or recording, misuse of personal devices, cyber threats, data breaches and other risks associated with digital technology.

As a British international school in the UAE, New Dawn Private School seeks to develop digitally responsible learners who understand their rights, responsibilities and the potential consequences of their online behaviour. The school promotes British Values, including democracy, the rule of law, individual liberty, mutual respect and tolerance of different faiths and beliefs, through its approach to digital citizenship and online conduct. These values are promoted in harmony with UAE laws, national identity, cultural expectations and the school's safeguarding responsibilities.

The school maintains a no-mobile-phone rule for learners. Personal mobile phones must not be used by learners during the school day, including lessons, breaks, lunch, school activities and school transport, subject to any specific written exception authorised by the school. Educational technology is provided and managed through approved school systems and devices.

The school adopts a preventative and educational approach to online safety, supported by clear rules, staff training, proportionate sanctions, parental partnership, effective monitoring and appropriate safeguarding action.

2. Purpose

The purpose of this policy is to establish a clear and consistent framework for the safe, secure, effective and responsible management and use of IT systems, software, hardware, networks, digital platforms and personal electronic devices across New Dawn Private School.

The policy aims to ensure that technology:

- Supports high-quality teaching, learning, assessment, communication and administration.
- Promotes digital literacy, innovation, creativity, collaboration and independent learning.
- Protects learners and staff from online harm, inappropriate content, exploitation, harassment, cyberbullying and other digital risks.
- Establishes clear expectations for the use of school-owned and personally owned devices.
- Enforces the school's no-mobile-phone rule for learners.
- Sets out appropriate sanctions and safeguarding responses for breaches of online safety and acceptable-use expectations.

This document has been approved by the School Management System

The only approved and controlled copy of this document is the one available electronically on the school's network. Printing and distributing of this document are prohibited. Users must verify the Revision Number and Issue Date of the document before use.

Page 3 of 28

- Protects confidential information, personal data, accounts, networks, systems and digital records.
- Prevents unauthorised photography, filming, audio recording, sharing of images and misuse of digital communication.
- Promotes respect, integrity, responsible decision-making and lawful digital conduct.
- Ensures that staff model safe and professional technology use.
- Supports inclusion and equitable access to appropriate digital learning.
- Ensures compliance with relevant UAE legislation, KHDA requirements and applicable regulatory standards.
- Supports continuous school improvement through monitoring, training, evaluation and the review of incidents.

3. Scope

This policy applies to all learners, staff, leaders, governors or proprietorial representatives where relevant, parents, volunteers, contractors, visitors and external providers who access or use the school's IT systems, digital platforms, devices, networks or information.

It applies on the school premises, during school transport, on educational visits, during school events, while participating in school-related online activities and whenever off-site digital behaviour affects the safety, welfare, reputation or orderly operation of the school.

The policy covers:

3.1 IT infrastructure and systems

School networks, Wi-Fi, servers, computers, laptops, tablets, interactive displays, printers, approved software, cloud services, digital learning platforms, accounts and administrative systems.

3.2 Educational technology

Technology used for teaching, learning, assessment, research, communication, digital literacy, coding, creativity and collaborative learning.

3.3 Administrative and operational technology

Systems used for admissions, attendance, assessment, reporting, safeguarding, communication, finance, HR, transport, records and school management.

3.4 Online safety and digital citizenship

Internet use, search engines, social media, messaging, gaming, artificial intelligence tools, email, online collaboration, digital reputation, cyberbullying, online exploitation, harmful content and responsible communication.

3.5 Personal devices

Mobile phones, smartphones, smartwatches, tablets, laptops, cameras, wearable devices, handheld gaming devices, audio recorders and any device capable of taking photographs, recording sound or video, accessing the internet, communicating with others or storing and transmitting data.

3.6 Cybersecurity and data protection

Passwords, authentication, phishing, malware, access controls, software updates, data storage, sharing, incident reporting, backups and the protection of personal and confidential information.

3.7 Monitoring, sanctions and review

Acceptable-use monitoring, incident reporting, investigation, sanctions, safeguarding referrals, staff training, quality assurance and continuous improvement.

This policy must be read alongside the school's Safeguarding and Child Protection Policy, Staff Code of Conduct, Behaviour Policy, Anti-Bullying Policy, Data Protection arrangements, Complaints Policy and relevant safeguarding, inclusion and health and safety procedures.

4. Policy Principles and British Values

4.1 Democracy

Learners are encouraged to participate responsibly in digital learning, communicate respectfully and understand that online platforms can provide opportunities for collaboration, debate and the sharing of ideas. Digital participation must not involve harassment, intimidation, discrimination, manipulation or the deliberate silencing of others.

4.2 The rule of law

Learners and staff must understand that online behaviour is subject to school rules and applicable laws. Unauthorised access, hacking, fraud, threats, harassment, harmful sharing of images, deliberate data breaches and other unlawful activities will be treated seriously and referred to competent authorities where required.

4.3 Individual liberty

The school supports responsible access to information, independent learning and informed decision-making. Individual liberty does not give anyone permission to misuse technology, violate another person's privacy, access harmful material, breach school rules or place others at risk.

4.4 Mutual respect

All users must communicate respectfully online and offline. Cyberbullying, humiliating content, threatening messages, discriminatory language, impersonation, malicious rumours and the unauthorised sharing of another person's information or images are prohibited.

4.5 Tolerance of different faiths and beliefs

Digital learning and communication must reflect respect for different faiths, beliefs, cultures, backgrounds and identities. Content that promotes hatred, extremism, religious intolerance, discrimination or deliberate offence is prohibited and will be addressed in accordance with school procedures and applicable UAE requirements.

4.6 UAE identity and culture

The school promotes responsible digital citizenship that respects UAE national identity, culture, traditions, laws and values. Technology must not be used to create, access, share or distribute material that breaches applicable UAE law or school expectations.

4.7 Inclusion and equal access

Digital technologies should support the participation and progress of all learners, including learners with additional learning needs, disabilities or language needs. Staff must consider accessibility, reasonable adjustments and the risks associated with digital participation when planning learning.

5. Acceptable Use of IT Systems

5.1 General expectations

All users must:

- Use school technology primarily for authorised educational, professional or operational purposes.
- Follow instructions from authorised staff and IT personnel.
- Use only accounts, systems, applications and platforms approved by the school.
- Keep passwords confidential and use appropriate authentication.
- Protect devices from loss, damage, theft and unauthorised access.
- Respect the privacy, dignity and intellectual property of others.
- Report suspicious messages, inappropriate content, cyberbullying, security weaknesses and suspected breaches promptly.
- Follow the school's safeguarding, confidentiality and data protection procedures.
- Use school systems in a way that supports learning, wellbeing and the effective operation of the school.

Users must not:

- Access another person's account or files without permission.
- Share passwords, authentication codes or access credentials.
- Attempt to bypass filtering, monitoring, access controls or security measures.
- Download or install unauthorised software, applications or browser extensions.
- Introduce malware, attempt hacking or interfere with school networks.
- Use school technology to bully, harass, threaten, discriminate against or impersonate others.
- Access, create, store or distribute illegal, sexually explicit, violent, extremist or otherwise inappropriate content.
- Use school systems for unauthorised commercial activity, gambling, unlawful activity or other prohibited purposes.
- Deliberately damage, alter, delete or disclose school information.
- Use technology to disrupt lessons or interfere with another user's work.

5.2 Educational use

Teachers must ensure that technology is used purposefully and supports the learning objective. Digital tools should enhance learning rather than replace effective teaching, discussion, practical experiences or direct interaction.

Teachers must:

- Select age-appropriate, curriculum-relevant and school-approved digital resources.
- Consider online safety before directing learners to websites, platforms or applications.
- Explain safe and responsible use before introducing unfamiliar digital tools.
- Supervise learners in accordance with their age, needs and the activity's level of risk.
- Check that digital content is appropriate for the intended learners.
- Provide accessible alternatives where necessary.
- Report inappropriate material, suspicious activity or misuse immediately.
- Ensure that technology use complies with assessment integrity and examination requirements.

5.3 Artificial intelligence and emerging technologies

AI tools may only be used in accordance with school guidance and approved educational purposes.

Users must not:

- Enter confidential learner, family, staff or school information into unapproved AI systems.
- Upload identifiable photographs, recordings, reports or personal data without appropriate authorisation.
- Use AI to generate threats, harassment, discriminatory content, impersonations or harmful deepfakes.
- Present AI-generated work as their own where this breaches assessment expectations.
- Rely on AI-generated information without appropriate verification.

Staff must check the suitability, accuracy, age appropriateness and privacy implications of AI tools before use. Learners must be taught to recognise that digital content can be misleading, manipulated or inaccurate.

6. Online Safety and Digital Citizenship

Online safety is the responsibility of all members of the school community. It is embedded in teaching, safeguarding, pastoral support, staff development and the school's wider culture.

6.1 Education and prevention

The school will provide age-appropriate teaching and guidance on:

- Protecting personal information and digital identity.
- Creating secure passwords and recognising phishing attempts.
- Identifying misleading information, scams and manipulated content.
- Cyberbullying, online harassment and respectful communication.
- Safe use of social media, messaging, gaming and online communities.
- Privacy settings, location sharing and digital footprints.
- Online grooming, exploitation, coercion and requests for inappropriate images.
- The risks of sharing photographs, videos, personal information and live location data.
- Appropriate use of AI, digital content and copyrighted material.
- Reporting unsafe online behaviour and seeking help from trusted adults.
- The legal and personal consequences of harmful or unlawful online conduct.

Teaching must be age-appropriate and sensitive to learners' developmental stages, needs and cultural context.

6.2 Internet filtering and monitoring

The school will implement appropriate technical and organisational safeguards to reduce exposure to harmful content and protect its systems.

These may include:

- Web filtering and access restrictions.
- Antivirus, endpoint protection and security updates.
- Access permissions and account controls.
- Monitoring of school networks and approved digital platforms.
- Restrictions on unauthorised downloads, applications and external storage.
- Review of security alerts and suspected misuse.

Filtering and monitoring are protective measures and do not replace supervision, education or safeguarding intervention. No filtering system can guarantee that all inappropriate material will be blocked.

Monitoring will be conducted for legitimate educational, safeguarding, security and operational purposes, proportionately and in accordance with applicable UAE law and data protection requirements. Users must not assume that activity on school systems is entirely private.

6.3 Social media and online communication

Learners must not use social media, messaging applications or online platforms to bully, threaten, impersonate, humiliate or target other members of the school community.

Staff must not communicate with learners through personal social media accounts or private messaging channels unless an explicitly authorised and compliant arrangement exists. Approved school communication channels must be used wherever possible.

Staff must not publish identifiable images, recordings or information about learners through personal accounts without appropriate school authorisation and consent where required.

Parents and visitors are expected to respect the privacy of learners and staff when posting online and must not publish images or recordings of other learners without appropriate permission.

6.4 Cyberbullying

Cyberbullying includes, but is not limited to:

- Repeated threatening, insulting or humiliating messages.
- Sharing embarrassing photographs, videos or personal information.
- Creating fake profiles or impersonating another person.
- Excluding or targeting someone through online groups.
- Spreading malicious rumours or discriminatory content.
- Threatening to publish private material.
- Encouraging others to harass, intimidate or harm a person.
- Using digital tools or AI to create harmful impersonations or manipulated content.

All reports will be taken seriously. The school will establish the facts, assess the safeguarding risk, support affected learners, contact parents where appropriate and apply proportionate consequences.

Online incidents that occur outside school may still require school intervention where they affect learner safety, wellbeing, attendance, relationships or the orderly operation of the school.

6.5 Inappropriate or harmful content

Users must not deliberately search for, create, store or distribute content that is illegal, exploitative, sexually explicit, violent, hateful, extremist or otherwise inappropriate for the school environment.

If a learner encounters harmful content, they should stop interacting with it, avoid forwarding it, and report it to a trusted member of staff.

Staff must not unnecessarily copy, download, forward or circulate suspected illegal or harmful material. Any potential safeguarding evidence must be handled in accordance with the school's safeguarding procedures and advice from the appropriate authority.

6.6 Reporting online safety concerns

Any learner or staff member who becomes aware of an online safety concern must report it promptly to a trusted teacher, Head of Key Stage, the Designated Safeguarding Lead (DSL), the Principal or the IT team, depending on the nature of the incident.

- **Safeguarding risk:** report immediately to the DSL or the designated alternative route.
- **Cyberbullying or harmful online behaviour:** report to the relevant pastoral or senior leader and the DSL where safeguarding concerns exist.
- **Cybersecurity incident:** report immediately to IT and the appropriate senior leader.
- **Lost or stolen device containing school information:** report immediately to IT and the relevant senior leader.
- **Suspected data breach:** report immediately through the school's data protection and incident reporting arrangements.

Staff must not promise secrecy where a learner discloses harm. The information must be shared with the appropriate person to safeguard the learner.

7. Learner Use of Mobile Phones, Cameras and Handheld Devices

7.1 No-mobile-phone rule

New Dawn Private School operates a **no-mobile-phone policy for learners**.

Learners are not permitted to use personal mobile phones during the school day. This includes lessons, corridors, toilets, breaktimes, lunchtime, assemblies, extracurricular activities and school events, unless a specific written exception has been authorised by the Principal for an identified purpose.

The school day includes the period from arrival on school premises until the learner has left the premises at the end of the school day. Learners travelling on school transport must also follow the school's device and behaviour expectations.

7.2 Bringing a phone to school

The school strongly expects learners not to bring mobile phones to school.

Where a phone is brought for an exceptional travel or family communication reason:

- The parent must ensure that the learner understands the school's rules.
- The phone must be switched off before entering the school environment and remain switched off and securely stored for the entire school day.

- The phone must not be used, displayed, accessed or carried in a way that disrupts school expectations.
- The school may require the phone to be handed to an authorised staff member or stored securely in accordance with school arrangements.
- The school accepts no responsibility for loss or damage to personal devices brought contrary to its expectations, subject to applicable legal obligations.

Parents who need to contact a learner during the school day must contact the school office. Learners who need to contact a parent must seek permission from an authorised member of staff.

7.3 Smartwatches and connected wearables

Smartwatches and wearable devices capable of messaging, calling, recording, photography, internet access or other communication must be switched off or have these functions disabled and remain inaccessible during the school day.

Where a device cannot reliably comply with this requirement, the school may require the learner not to bring it to school.

A medical or accessibility device required to support a learner's needs may be permitted through a written arrangement agreed with the Principal and relevant staff. Such arrangements must identify the permitted functions, supervision requirements and safeguards.

7.4 Cameras, photography and recording

Learners must not use personal or school devices to photograph, film or record other learners, staff, visitors or school activities unless a member of staff has explicitly authorised the activity for an approved educational purpose.

Learners must never:

- Photograph or record another person in toilets, changing areas or other private spaces.
- Record conversations without appropriate authorisation.
- Photograph, film or share images of a person in a humiliating, threatening or compromising situation.
- Upload or distribute images, videos or recordings of other learners or staff without appropriate permission.
- Use a device to capture safeguarding, medical, disciplinary or confidential information.
- Create or share manipulated images, deepfakes or AI-generated content intended to impersonate, harass or harm another person.

Authorised educational photography must be undertaken under staff supervision and in accordance with school procedures, consent arrangements and data protection requirements.

7.5 Gaming devices and other handheld devices

Personal gaming consoles, tablets, cameras, audio recorders and other handheld electronic devices must not be used during the school day unless specifically authorised by a member of staff for an approved educational or accessibility purpose.

Devices must not be used to access games, social media, messaging, inappropriate content or unauthorised internet services during school activities.

7.6 Consequences for learner device misuse

Where a learner breaches this section, the school will respond proportionately, taking account of age, intent, impact, previous incidents, additional needs and safeguarding considerations.

Possible sanctions include:

1. A reminder of expectations and immediate cessation of the activity.
2. Confiscation of the device for secure storage until the end of the school day, in accordance with school procedures.
3. Recording the incident and informing the parent.
4. A behaviour sanction in line with the Behaviour Policy.
5. A parent meeting and an agreed digital safety improvement plan.
6. Temporary restrictions on access to school IT systems or devices, where appropriate.
7. Escalated behaviour sanctions for repeated or serious misuse.
8. A safeguarding investigation and referral to the DSL where required.
9. Referral to competent UAE authorities where the behaviour may involve unlawful activity or a serious safeguarding risk.

Phones and other devices must be handled securely and respectfully. Staff must not search the contents of a personal device without appropriate authority and a lawful, school-approved basis. Any urgent safeguarding concern must be managed through the safeguarding procedure.

8. Staff Use of Phones, Cameras and Handheld Devices

8.1 Professional expectations

Staff must model safe, professional and responsible use of technology. Personal devices must not distract from supervision, teaching, safeguarding, professional duties or interactions with learners.

During lessons, duties, meetings, supervision and other learner-facing responsibilities, staff must not use personal phones for non-work purposes except where authorised or required by an emergency, medical need or agreed reasonable adjustment.

Staff should keep personal phones securely stored and on silent during teaching and supervision, unless an approved work-related arrangement requires otherwise.

8.2 Personal communication

Staff must not use personal phones to communicate privately with learners through calls, text messages, social media or messaging applications, except where a specific arrangement has been formally authorised by the school and complies with safeguarding requirements.

School-approved communication systems must be used for school business wherever possible. Staff must not share personal contact details with learners for informal communication or encourage learners to contact them through personal accounts.

8.3 Photography, filming and audio recording

Staff must not use personal phones or personal cameras to photograph, film or record learners for school purposes.

Learner images and recordings must be captured using school-approved equipment and stored or transferred through approved school systems. Staff must follow consent arrangements, data protection requirements and school guidance concerning the use and publication of images.

Staff must not:

- Photograph or record learners on personal devices.
- Store learner images, videos or recordings in personal galleries, personal cloud storage or personal messaging accounts.
- Share images or recordings through personal social media.
- Record confidential conversations or meetings without appropriate authorisation.
- Photograph confidential documents, learner records or safeguarding information on personal devices.
- Use personal devices in toilets, changing areas or other sensitive locations in a manner that compromises privacy or safeguarding.

If an emergency makes use of a personal device unavoidable, staff must inform the Principal or appropriate senior leader as soon as possible, transfer any necessary information through an approved secure process and delete any unauthorised local copy once its retention is no longer necessary and lawful. Safeguarding evidence must not be deleted or altered; staff must seek direction from the DSL or appropriate authority.

8.4 School-issued phones and handheld devices

School-issued phones, tablets, cameras and other handheld devices may be used only for authorised professional, educational, operational or safeguarding purposes.

Staff must:

- Protect devices with appropriate security controls.
- Keep devices in their possession or in an approved secure location.

This document has been approved by the School Management System

The only approved and controlled copy of this document is the one available electronically on the school's network. Printing and distributing of this document are prohibited. Users must verify the Revision Number and Issue Date of the document before use.

Page 13 of
28

- Report loss, theft, damage or suspected compromise immediately.
- Avoid using devices to access personal or unauthorised services.
- Ensure that photographs, recordings and data are transferred to approved systems.
- Return devices and accessories when requested or when their role ends.

8.5 Staff use of phones during emergencies

A personal phone may be used where necessary to contact emergency services or respond to an immediate safeguarding or health and safety concern if approved communication systems are unavailable or unsuitable.

Staff must inform the appropriate senior leader as soon as practicable and record the incident through the relevant school procedure.

8.6 Consequences for staff misuse

A breach of this policy may result in:

- An informal reminder or management instruction for a minor, inadvertent breach.
- A formal record of concern and required refresher training.
- Restriction or removal of access to school systems or devices.
- A formal investigation under the Staff Code of Conduct or disciplinary procedure.
- Referral to the DSL and safeguarding procedures where learner safety may be affected.
- Referral to competent UAE authorities where required.

Serious misconduct, unauthorised recording, inappropriate communication with learners, deliberate disclosure of confidential information or conduct that places learners at risk may require immediate protective measures and formal investigation. Any action must follow the school's approved procedures and applicable law.

9. Online Safety Sanctions and Response Framework

The school recognises that online safety incidents range from accidental misuse to serious and potentially unlawful behaviour. Responses must be proportionate, consistent and focused on safeguarding, accountability, education and the prevention of recurrence.

The following framework provides indicative responses. It does not prevent the school from taking more urgent or serious action where the circumstances require it.

Level 1: Low-level or first-time misuse

Examples may include:

- Accessing an unrelated website during a lesson.
- Attempting to use a personal device contrary to school rules without aggravating circumstances.

- Minor misuse of an approved digital platform.
- An accidental breach of acceptable-use expectations.

Possible responses:

- Immediate instruction to stop the activity.
- Verbal reminder and reteaching of the relevant rule.
- Temporary restriction of the relevant activity.
- Recording where appropriate.
- Parent communication where repeated or necessary.

Level 2: Repeated or deliberate misuse

Examples may include:

- Repeated use of a phone or unauthorised device.
- Deliberately bypassing filtering or access restrictions.
- Sending inappropriate messages or using school platforms inappropriately.
- Repeated cyberbullying or targeted online harassment.
- Unauthorised sharing of photographs or recordings.
- Deliberately accessing unsuitable content.

Possible responses:

- Formal behaviour sanction.
- Confiscation and secure storage of a device, where appropriate.
- Parent notification and meeting.
- Restriction of access to specific IT systems or privileges.
- Digital safety education or a behaviour improvement plan.
- Referral to the DSL where the incident indicates a safeguarding concern.

Level 3: Serious, harmful or potentially unlawful misuse

Examples may include:

- Threats, intimidation, targeted harassment or serious cyberbullying.
- Creating or sharing humiliating, sexually explicit or manipulated images.
- Unauthorised recording in private or sensitive spaces.
- Sharing confidential, personal or safeguarding information.
- Attempts to hack accounts, steal credentials or deliberately compromise school systems.
- Online grooming, exploitation, coercion, blackmail or threats to distribute private material.
- Accessing, creating or distributing illegal material.
- Conduct that presents a serious risk to a learner's safety or wellbeing.

Possible responses:

- Immediate safeguarding assessment and protective action.
- Immediate restriction of relevant access or devices where necessary.
- Formal investigation under the Behaviour Policy, Staff Code of Conduct or relevant procedure.
- Parent notification, where appropriate and safe.
- Serious behaviour sanctions, which may include suspension or a recommendation for further disciplinary action in accordance with school policy and applicable requirements.
- Referral to competent UAE authorities where required.
- Preservation of relevant evidence and secure incident records.
- Support for affected learners and review of the risk of further harm.

A serious incident does not need to progress through Levels 1 and 2 before action is taken.

9.1 Factors considered when deciding sanctions

The school will consider:

- The age, maturity and individual needs of the learner.
- Whether the behaviour was accidental, reckless or deliberate.
- The nature and severity of the content or conduct.
- The impact on the affected person and the wider school community.
- Whether the incident involved threats, coercion, discrimination, exploitation or a safeguarding risk.
- Whether the learner has previously breached the policy.
- Whether the learner accepted responsibility and engaged with restorative or educational action.
- Whether reasonable adjustments or additional support are appropriate.

Sanctions must be fair, proportionate and consistent with the school's Behaviour Policy and applicable UAE requirements. A learner's additional needs must be considered without diminishing the school's duty to protect others.

9.2 Confiscation and inspection of devices

Authorised staff may require a learner to hand over a device where there is a reasonable school-related basis, such as a breach of the no-phone rule or a safeguarding concern. The device must be stored securely and returned in accordance with the school's procedures.

Staff must not routinely browse the contents of a personal phone or handheld device. Any proposed examination of device contents must be justified, proportionate and authorised through the appropriate school procedure, with regard to privacy, safeguarding and applicable law.

Where there is a concern involving potentially illegal material, exploitation or serious harm, staff must not circulate or unnecessarily handle the material. They must seek immediate guidance from the DSL and, where required, the appropriate UAE authority.

9.3 Restorative and educational responses

Where appropriate, the school may require a learner to complete digital citizenship education, reflect on the impact of their actions, agree a behaviour improvement plan or participate in a restorative process.

Restorative approaches must never require a victim to meet or reconcile with another learner where doing so would be unsafe, coercive or inappropriate.

10. Cybersecurity and Data Protection

10.1 Passwords and accounts

Users must protect their login credentials and must not share passwords or authentication codes. Staff must follow approved account security and access-control procedures.

Suspected account compromise must be reported immediately to IT and the relevant senior leader. Passwords must be changed and access secured in accordance with IT instructions.

10.2 Phishing, malware and suspicious communications

Users must not open suspicious links or attachments, enter credentials into unverified websites or install unapproved software.

Suspicious emails, messages, files or login requests must be reported promptly. Staff must not forward suspicious material unnecessarily.

10.3 Data handling

Personal and confidential information must only be accessed by authorised individuals for legitimate purposes. Information must be stored, transmitted and disposed of securely.

Staff must not use personal email accounts, unauthorised cloud storage or personal messaging applications to transfer confidential learner, parent or staff information.

10.4 Data breaches

Any suspected loss, unauthorised access, disclosure, alteration or destruction of personal or confidential data must be reported immediately through the school's approved incident reporting process.

The school will assess the incident, contain the risk, preserve relevant records, investigate the cause and make any required notifications in accordance with applicable UAE law and regulatory requirements.

10.5 System maintenance

The IT team will oversee appropriate maintenance, security updates, backups, access permissions and technical controls. Users must not disable, bypass or interfere with security measures.

11. Roles and Responsibilities

11.1 Principal and senior leadership team

The Principal and senior leadership team are responsible for:

- Implementing and reviewing this policy.
- Ensuring that online safety is integrated into safeguarding and school improvement.
- Ensuring that staff understand their responsibilities.
- Overseeing serious incidents and ensuring appropriate escalation.
- Ensuring sanctions are proportionate and consistent.
- Reviewing trends and ensuring that corrective actions are implemented.
- Providing appropriate information to the Proprietor or governance body.

11.2 Designated Safeguarding Lead

The DSL is responsible for:

- Receiving and assessing online safety concerns that may involve harm or exploitation.
- Coordinating safeguarding responses and referrals.
- Ensuring that staff understand reporting expectations.
- Working with senior leaders and IT to manage digital risks.
- Ensuring that relevant records are maintained securely.
- Ensuring that the school's response prioritises learner safety and wellbeing.

11.3 IT team

The IT team is responsible for:

- Maintaining and securing school IT infrastructure.
- Managing authorised accounts, permissions and systems.
- Implementing appropriate filtering and security controls.
- Supporting investigation of technical incidents.
- Maintaining appropriate logs and records.
- Advising staff on safe and approved technology use.
- Reporting significant risks to the Principal and DSL as appropriate.

11.4 Teachers and other staff

Staff are responsible for:

- Modelling responsible digital behaviour.
- Supervising learners' technology use appropriately.
- Teaching and reinforcing online safety expectations.
- Reporting concerns and suspected breaches promptly.
- Using approved systems for communication and data handling.
- Protecting learner privacy and confidentiality.
- Following the Staff Code of Conduct and safeguarding procedures.

11.5 Learners

Learners are responsible for:

- Following the school's acceptable-use and no-mobile-phone rules.
- Treating others respectfully online and offline.
- Protecting their accounts and personal information.
- Avoiding harmful, inappropriate or unlawful content and behaviour.
- Reporting concerns to a trusted adult.
- Following staff instructions regarding devices and digital activities.

11.6 Parents and carers

Parents and carers are expected to:

- Support the school's no-mobile-phone rule and acceptable-use expectations.
- Discuss online safety and responsible device use with their children.
- Notify the school of significant online incidents affecting learner safety or school life.
- Use appropriate communication channels when contacting learners during the school day.
- Respect the privacy of other learners and staff when taking or sharing photographs and recordings.
- Work constructively with the school when concerns arise.

12. Staff Training and Learner Education

The school will provide relevant induction and refresher training so staff understand:

- Acceptable use of IT systems and personal devices.
- Online safety and safeguarding risks.
- Reporting and escalation procedures.
- Cybersecurity, phishing and data protection.
- Appropriate communication with learners.
- Photography, recording and image-sharing requirements.
- The use of sanctions and the preservation of evidence.
- The relationship between this policy, safeguarding and the Staff Code of Conduct.

Online safety education will be incorporated into relevant curriculum areas, pastoral sessions, assemblies and digital learning. Learners will be encouraged to ask for help, report unsafe behaviour and understand that seeking support is the right action.

The school will provide appropriate information to parents about online safety risks, the no-mobile-phone rule, reporting concerns and the school's response to breaches.

13. Monitoring, Recording and Quality Assurance

The school will monitor the implementation and effectiveness of this policy through:

- Review of online safety and IT incident records.
- Analysis of sanctions, repeat incidents and patterns of behaviour.
- Review of cyberbullying, device misuse and unauthorised recording concerns.
- Checks of filtering, access controls and technical safeguards.
- Learner, staff and parent feedback where appropriate.
- Review of staff training and learner digital citizenship education.
- Safeguarding reviews and leadership oversight of serious incidents.
- Evaluation of the impact of corrective and preventative actions.

Significant incidents must be recorded through the appropriate behaviour, safeguarding, IT or data protection systems. Where an incident crosses more than one area, records should be linked or cross-referenced securely to ensure that relevant leaders can coordinate the response.

The school will use the cycle:

Risk identified → Action taken → Evidence reviewed → Impact evaluated → Improvement

14. Terms and Definitions

The following Terms and Acronyms are used within this document and are defined as follows:

Term / Acronym	Definition
SIS	Student Information System
MDM	Mobile Device Management
JAMF	Jamf Apple Device Management
Information Technology (IT)	The use, management, and maintenance of digital systems, devices, software, networks, and technological resources to support teaching, learning, communication, administration, and school operation
Hardware	Physical technological equipment used within the school, including computers, laptops, tablets, printers, servers, projectors, interactive screens, routers, and other devices.
Software	Programs and digital applications used for educational, administrative, operational, or communication purposes

Network	The school's wired and wireless communication systems that allow devices and users to connect, share information, and access digital resources and the internet.
Educational Technology (EdTech)	Digital tools and platforms used to enhance teaching, learning, assessment, collaboration, and student engagement.
User Account	A secure digital identity assigned to staff or students to access school systems, networks, platforms, and applications.
Data Protection	The process of safeguarding personal, confidential, and school-related information to ensure privacy, security, and compliance with regulations
IT Infrastructure	The overall technological framework of the school, including hardware, software, networks, servers, internet connectivity, and digital systems.

6- Procedures:

6.1 For staff and employees

- 1-Design and print staff/employee ID card based on shared details by HR.
- 2-Register and configure school buildings access doors using ZKAccess3.5 Security System.
- 3-Handover the teachers lanyard for ID and access door cards.
- Configure face/ Fingerprint on the biometric machine for attendance.
- Create Microsoft 365 account including email based on HR shared details.
- Add staff to the designated email group based on his/ her position for easy and targeted communication.
- Add staff to the designated school Drive/ SharePoint based on position and responsibilities.
- Add staff to the designated TEAMs channel based on position and responsibilities.
- Add staff to the Teaching Module on ISAMS school system.
- Add staff to the designated school WhatsApp group and channels.
- Add staff to all School approved and active applications such as Dojo/Teams SharePoint GL Assessments and internal external platforms.
- Familiarise the employee with the required skills for logging in and accessing school applications and platforms.
- Conduct group/ one to one based on needs training on using classroom Smart Boards/ Applications and platforms / school system

Configure the staff/ employee to school personal and school devices to the school network access.

15-Share with the staff member through an email the list of Key Person communication details (Form 002)

6.2 For students and parents

- 1-Design and print students/parent ID card based on shared details by admission.
- 2- Handover ID cards and lanyards to students and parents.
- 3- Create Microsoft Teams account based on shared details by admission.
- 4- Add student to the designated teams class channel based on shared details by admission.
- 5- Add student to the designated Class dojo system based on shared details by admission.
- 6- Add student to all School approved and active applications such as Dojo/Teams GL Assessments Kutubee Raz Kids and internal external platforms.

6.3 IT Infrastructure Management

- Daily monitor network performance and connectivity
- Daily ensure Wi-Fi, servers, and systems are operational
- Daily check backup systems status
- Weekly perform system health checks
- Review storage and performance
- Update software and security tools
- Termly conduct full IT audit (hardware & software)
- Termly plan upgrades and improvements

6.4 Systems Management

Manage and monitor the following systems:

Microsoft 365) SharePoint, OneDrive, Outlook, Forms, Sway)

- **Create and manage user accounts and permissions**
- **Support communication (Outlook and Teams)**
- **Manage file storage and sharing (OneDrive, SharePoint)**
- **Setting up Teams for classes and add teachers and students for collaboration**
- **Create and maintain Forms.**

GL Assessment (NGRT, CAT4, PTE, PTS, PTS, and PASS.)

- **Create student and staff users based on students' admission list.**
- **Create and manage teacher accounts.**
- **Keep the system updated.**
- **Administer user accounts (add, edit, remove, deactivate).**

Microsoft Teams System

- Create and manage student accounts.
- Create and manage teacher accounts.
- Create classes and channels.
- Assign teachers and students to classes.
- Support communication and collaboration through Teams.

School SharePoint

- Create and manage SharePoint sites and pages.
- Create and organise files and document.
- Upload and maintain school resources and materials.
- Add teachers and staff users.
- Assign roles and manage permissions (access control).
- Manage folder structure and ensuring secure file sharing.

ClassDojo system

- Create and manage classes.
- Create teacher accounts and assign teachers to classes.
- Create and manage student accounts.
- Add and manage parent accounts for communication.
- Manage parent-teacher communication through the platform.
- Assign roles and permissions.
- Moving students between classes when required.

Apple School Manager

- Manage Apple School Manager accounts and settings.
- Enroll and configuring iPads for students and teachers.
- Create and manage Apple IDs for staff and students.
- Assign devices to users and classes.
- Manage apps and device permissions through MDM integration.
- Support iPad setup, troubleshooting, and updates.

iPad JAMF Apple School

- Manage iPads through JAMF MDM system.
- Enroll and configure student and teacher iPads.
- Deploy and manage applications (install, update, remove).
- Apply security policies, restrictions, and device permissions.
- Manage device profiles, Wi-Fi settings, and configurations.
- Monitor device compliance and troubleshooting iPad issues.
- Support integration with Apple School Manager.

Firewall server security

- Manage and configure firewall security policies and rules.
- Monitor network traffic and ensuring secure internet access.
- Control user access and applying content filtering.
- Manage VPN access and secure remote connections.
- Implement server security measures and access control.
- Perform system monitor, patching, and security updates.
- Ensure data protection, backup, and disaster recovery readiness.

CCTV Camera system

- Manage and monitor the school CCTV surveillance system.
- Configure cameras, NVR/DVR record settings, and storage.
- Create and manage user access and permissions.
- Troubleshoot camera connectivity and record issues.
- Maintain CCTV system performance and ensure continuous monitor.
- Support incident review by retrieving and exporting video footage when required.

Printer software system.

- Manage and configure network printers and printing software.
- Install and update printer drivers and applications.
- Monitor printer status, usage, and performance.
- Troubleshoot print, scan, and connectivity issues.
- Manage print queues and resolving user printing requests.
- Ensure secure and efficient printing across the school network.
- Provide user access and permissions as per management request.
- Order and manage printer consumables (toner, paper, and supplies).

Promethean smart Board software. (Share screen)

- Install and manage Promethean interactive board software.
- Support classroom screen sharing and interactive teaching tools.
- Connect devices and ensure smooth display integration.
- Troubleshoot software and connectivity issues.
- Update software and maintain system performance.
- Support teachers in using smart board features effectively.
- Provide training and guidance to teachers on smart board usage.

NDPS WhatsApp Channels

- Create and manage official school WhatsApp channels.
- Post announcements, updates, and important notifications with pastorals team.
- Share events, reminders, and school communications.
- Manage channel settings and subscriber access.
- Ensure timely and accurate information delivery to parents and staff.
- Support school communication and engagement through WhatsApp platform.

ZKTeco Biometric System (Staff attendance)

- Manage and configure the ZKTeco biometric attendance system.
- Enroll and maintain staff fingerprint/face data.
- Monitor daily staff attendance and generating reports.
- Troubleshoot device and software connectivity issues.
- Ensure accurate attendance tracking and system reliability.
- Support HR and management with attendance data and records.

TES Safeguarding system.

- Manage and configure the TES Safeguarding Platform.
- Create and maintain user accounts for staff access.
- Ensure secure handling of sensitive student and staff information.
- Support reporting and compliance with safeguarding policies.
- Provide access permissions as per school safeguarding requirements.
- Assist staff with system usage and troubleshooting issues.

NDPS Website

- Update and managing website content.
- Upload and updating school photos for SLT members.
- Support school announcements, news, and event updates.
- Coordinate with the website developer to edit, remove, or add required content and page

NDPS Social media

- Manage and update the school's social media platforms with head of social media Ms Houda.
- Create and publish posts, announcements, and event updates on Instagram Facebook and LinkedIn school page.
- Upload and edit photos and media content.
- Support school marketing and community engagement online.
- Monitor messages comments and responding to inquiries when required.

Access Door Cards (ZKAccess3.5 Security System)

- Manage and administer door access cards using ZKAccess3.5.
- Issue, activate, deactivate, and update staff access cards.
- Troubleshoot access control issues (card not working, door access errors, device offline).
- Replace lost/damaged cards and ensure proper access control compliance.

Times Table Rock Stars (TTRS)

- Manage and administer the Times Table Rock Stars platform.
- Create, update, and maintain student and teacher accounts.
- Organise classes/groups and assign access to students.
- Support teachers with setup, training, and troubleshooting.

Kutubee (Digital Library / eBooks Platform)

- Manage and administer the Kutubee platform for students and staff.
- Create and maintain user accounts and access permissions.
- Support teachers and students with login and usage issues.

Wayground System & Twinkl

- Manage and support the Wayground and Twinkl platforms for teachers and students, including account setup, access management, troubleshooting, and coordination with vendors/management for updates, subscriptions, and renewals, while also providing ongoing assistance and basic training to ensure effective use of the platforms.

6.5 Digital Safeguarding & Online Safety

- Ensure safe use of all platforms
- Enforce meeting rules (teachers as organizers)
- Maintain filtering and security systems

6.6 Teaching & Learning Support

This document has been approved by the School Management System

The only approved and controlled copy of this document is the one available electronically on the school's network. Printing and distributing of this document are prohibited. Users must verify the Revision Number and Issue Date of the document before use.

Page 26 of
28

- Ensure classroom technology is functional
- Support teachers with digital tools
- Provide training on:
 - Microsoft Teams
 - systems platforms
 - Smartboard safeguarding
 - SharePoint

6.7 Data Protection & Security

- Ensure compliance with data protection policies
- Control access to sensitive data
- Backup Procedures
- Daily automated backups in OneDrive.
- Incident Management
- Investigate and document incidents

7-Accountability

The IT Manager is accountable for:

- Ensuring all IT systems are operational, secure, and aligned with school policies
- Maintaining confidentiality, integrity, and availability of data
- Delivering timely technical support and minimizing disruption to teaching and learning
- Ensure compliance with digital safeguarding and data protection regulations
- Reporting system performance, risks, and incidents to Senior Leadership Team (SLT)

8-Policy Review

This Procedures Manual will be reviewed:

- Annually as part of the school's policy review cycle
- Following any major changes in systems, infrastructure, or regulatory requirements (e.g., KHDA guidance)
- After significant incidents (e.g., data breaches, system failures)
- The IT Manager is responsible for initiating the review, with input from the Senior Leadership Team (SLT).
- All updates must be documented, approved by SLT, and communicated to relevant stakeholders.

9-Related Forms and Documents

- Staff handbook.
- Safeguarding policy
- Cyber security policy
- iPad Use policy
- CCTV Camera policy
- IT Asset Register
- Backup Logs
- Training Records