ISCA
INTERNATIONAL SCHOOL OF CREATIVE ARTS

International School of Creative Arts

E-safety Policy

Need a large print copy?

Please ask in the School Office.

ISCA

INTERNATIONAL SCHOOL OF CREATIVE ARTS

Control Page

Document Title	E-safety Policy	
Document Reference	ISCA 17	
Version	5.2	050/08/2024
Author	Executive Director	
Location	J:\9. POLICIES AND PROCEDURES\Approved	
Controller	Head of School	
Approved by	Senior Management Team	
Date of Adoption	September 2024	
Date of Next Review	September 2025	

Contents

Policy Statement

Background

The School recognises that Information Technology (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge students, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the School community. However, it is important that the use of IT and the Internet is understood and that it is the responsibility of students and staff, to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Scope

E-safety does not just cover the Internet and available resources, but all different types of devices and platforms (e.g. smartphone devices, wearable technology and other electronic communication technologies). The School understands that some adults and young people will use these technologies to harm children. The School has a 'duty of care' towards any staff, students or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who are given access to the school's IT systems. This could include staff, directors and students. However, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the student.

Purpose

This policy aims to be an aid in regulating IT activity in School, and provide a good understanding of appropriate IT use that members of the School community can use as a reference for their conduct online outside of school hours. E-safety is a whole school issue and responsibility.

Cyberbullying by students will be treated as seriously as any other type of bullying and will be managed through the School's anti-bullying policy and procedures.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

This policy should be read in conjunction with other material listed in Appendix 1.

Mandate

Roles and responsibility

The Head of School, Designated Safeguarding Lead, Head of Operations, IT Technical Support and Board of Directors will ensure that the e-safety policy is implemented and that compliance with the policy is monitored. The day-to-day management of e-safety in the School is the responsibility of IT Technical Support. They will work closely with the Head of Operations and senior academic staff in this regard.

The Board of Directors will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

Communicating School policy

All individuals issued access to the School's IT will be inducted into the e-safety policy and this policy is available on the School website for all to access, when and as they wish. Rules relating to the School Code of Conduct when online, and e-safety guidelines, are displayed around the School. E-safety is integrated into the curriculum in any circumstance where the Internet or technology is being used, as well as being specifically addressed in the PHSE curriculum. On joining the School, new students and staff are required to agree to the Staff or Student code of conduct, which covers IT acceptable practice. Existing staff may on occasion be required to re-sign this policy when significant changes are made.

Making use of IT and the Internet in School

Using IT and the Internet in School brings many benefits to students, staff and parents. The Internet is used to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a large part of everyday life, education and business. The School will endeavour to equip students with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave ISCA.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students, (some age specific). The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer or device connected to the School network. The School cannot accept liability for the material accessed, or any consequences of internet access unless found to be negligent.

Expectations of use of School computers apply to staff and students both in and out of lessons.

Learning to evaluate Internet content

With so much information available online, it is important that students learn how to evaluate Internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
- to acknowledge the source of information used and to respect copyright. The School will take any intentional acts of plagiary very seriously;
- about the risks associated with using the Internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;

- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

The School provides e-safety guidance to staff to better protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

If staff or students discover unsuitable sites then the URL, time, date and content must be reported to the IT Support Officer or any member of staff. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via a member of the Senior Management Team. Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

Managing information systems

The School is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of School data and personal protection of the School community seriously. This means protecting the School network, (as far as is practicably possible), against viruses, hackers and other external security threats.

The security of the School information systems and users will be reviewed regularly by the IT Support team and other third parties engaged with the School and led by the IT Support Officer. Anti-Virus and Malware protection software will be updated regularly. Some safeguards that the School takes to secure computer systems are:

- Making sure that unapproved software is not downloaded or installed to any School computers. Files held on the School network will be regularly checked for viruses;
- The use of user logins and passwords to access the School network will be enforced and unique.
- Portable media containing School data or programmes will not be taken off-site without specific permission from the Data Protection Officer (Head of Operations).
- Blocking access in inappropriate sites (see section on ‘Filtering and Monitoring’ for details)

For more information on data protection in the School, please refer to the School’s Data Protection and information security Policy, which can be accessed on the School’s website. More information on protecting personal data can be found later in this policy.

Filtering and Monitoring

In order to limit pupil’s exposure to the risk of harm from the internet deriving from the school’s IT system, ISCA has appropriate filtering and monitoring systems in place aimed at blocking harmful and inappropriate content without unreasonably impacting teaching and learning.

Our filtering and monitoring systems meet our safeguarding standards and are informed by the number and age range of our pupils, the needs of those who are potentially at greater risk of harm and how often pupils access the IT system (see Appendix 4 for details about the configuration).

We review the effectiveness of filtering and monitoring provision at least annually.

School leadership, the Designated Safeguarding Lead, IT Support and other relevant staff are trained to have an awareness and understanding of the provisions in place, to manage them effectively and to know how to escalate concerns when identified. In particular:

A Designated Member of the Board has strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

The Head of School is responsible for ensuring standards are met and:

- Liaising with the Landlord to for the procurement of suitable filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of provision and writing reports
- Ensuring that all staff:
    - understand their role
    - are appropriately trained
    - follow policies, processes and procedures
    - act on reports and concerns

The Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

Our IT Service Provider (IT Support) has technical responsibility for liaising with the DSL and our Landlord's IT provider to ensure:

- filtering and monitoring systems are maintained
- filtering and monitoring reports are provided
- actions are completed following concerns or checks to systems

Emails

The School uses email internally for staff and students, and externally for contacting parents, and conducting day to day school business and is an essential part of School communication.

Access in School to external personal email accounts may be blocked. The School has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use.

School email accounts and appropriate use

Staff should be aware of the following when using email in School:

- Staff should use their School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from School email accounts should be professional and carefully

written. Staff are representing the School at all times and should take this into account when entering into any email communications.

- The School permits the incidental use of staff School email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the School nor should it include or refer to anything which may bring the School into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any member of staff has breached these requirements, disciplinary action may be taken.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by the Head of School.
- Staff must tell the Head of School or a member of the Senior Management Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in School.
- The School will immediately disable email accounts of staff upon termination of employment.

Students should be aware of the following when using email in School:

Students will be taught to follow these guidelines at induction and in any instance where email is being used within the curriculum or in class:

- All students are provided with a School email account and students may only use approved email accounts for school purposes.
- Students are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases, will be restricted.
- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The School will disable student email accounts six months after leaving the School.

Published content and the School website

The School website is viewed as a useful tool for communicating School ethos and practice to the wider community. It is also a valuable resource for prospective parents and students, current parents, students and staff for keeping up-to-date with School news and events, celebrating whole-school achievements, personal achievements and promoting the School.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and transparency policies.

A team of staff, under the leadership of the Executive Director, are responsible for publishing and maintaining the content of the School website. The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright. Staff and students will be made aware of copyright in respect of material taken from the internet.

Staff and Students should take care not to publish anything on the Internet that might bring the School into disrepute. Any student or member of staff is welcome to discuss material with the Executive Director.

Policy and guidance of safe use of children's photographs and work

Colour photographs and students' work bring the School to life, showcase students' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of students and staff will not be displayed in public, either in print or online, without consent, if the use of the image is considered by the School to be privacy intrusive. Whether consent is obtained from the parents or the student themselves will depend upon the age and/or maturity of the student.

Using photographs of individual children

Most people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images.

Children may not be approached or photographed while in School or doing School activities without the School's permission, except for parents taking photographs or videos at School events involving their son or daughter for personal use only.

The School follows general rules on the use of photographs and videos of individual children:

- Consent will be obtained from either the parents or the student themselves (as appropriate) before using images in a way which is privacy intrusive. This may include images in:
  - School publications
  - on the School website
  - videos made by the School or in class for School projects.
- Electronic and paper images will be stored securely.
- Staff will only use equipment provided or authorised by the School, **(not their own device).**
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (e.g. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child without the consent of the parents or the child (as appropriate). Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as School drama productions or sports events must be used for personal use only

and are not to be posted on-line to platforms such as, but not limited to Facebook, Instagram and YouTube

- Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the students.

Complaints of misuse of photographs or video

Parents should follow standard School complaints procedure if they have a concern or complaint regarding the misuse of School photographs. Please refer to the Complaints Procedure for more information on the steps to take when raising a concern or making a complaint. Any issues or sanctions will be dealt with in line with this policy.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bullet-in boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that the School educates students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits. However, both staff and students should be aware of how they present themselves online. Students are taught through the induction and the PSHE curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place, (often referred to as a “digital tattoo”). The School follows general rules on the use of social media and social networking sites in School:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. Students are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School’s code of conduct regarding the use of IT technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official School blogs created by staff or students / year groups /School clubs as part of the School curriculum will be moderated by a member of staff and must be registered only against a School controlled email account.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and students to remember that they are always representing the School and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the Staff Handbook.
- Students and staff are not permitted to use VPN or other technology to circumvent

security features put in place by the School or its partners

Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make students and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The School's expectation is that mobile devices will be used responsibly at all times and certain measures are taken to ensure that staff and students adhere to this expectation. See our Mobile Phone Policy for further information.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the School. Information about specific strategies to prevent and tackle bullying are set out in the School's Anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Any incidents of cyberbullying will be dealt with in accordance with the School's Behaviour Policy, Anti-bullying policy and, where appropriate, the School's safeguarding and child protection policies and procedures.

Youth Produced Sexual Imagery

The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided equipment or personal equipment.

We will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so;
- send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our child protection policy;
- store the device securely;
- if an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image;
- carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies;
- inform parents/carers, if appropriate, about the incident and how it is being managed
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support;
- implement appropriate sanctions in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible;
- delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School, and will consider any educational and pedagogical benefits that they might have. The School keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting personal data

The School believes that protecting the privacy of staff, students, and parents and regulating their safety through data management, control and evaluation is vital to the whole school and individual progress. The School collects personal data from students, parents, and staff and processes it in accordance with the Data Protection Policy.

Related Documentation

This policy should be read in conjunction with the following policies and publications.

- Student Handbook
- Staff Handbook
- Staff Code of Conduct
- Student Code of Conduct
- Data Protection Policy
- Anti-Bullying Policy
- Keeping Children Safe in Education (September 2016)
- Behaviour Policy
- Mobile Phone Policy
- Complaints Procedure

Appendix 1

Device and technology acceptable use agreement for pupils

At International School of Creative Arts (ISCA), we know that using technology is an important part of your learning experience. We want everyone to be able to use technology, like the internet and laptops, but it is important that you are safe when you are using technology.

This agreement will set out the rules around using technology and devices, such as laptops and phones, when you are at school. Please read this document carefully and go through it with your parent. Once you are sure that you understand the rules set out in the agreement, please sign your name at the bottom.

If you have any questions about anything in this agreement, speak to your tutor.

Definitions

Before you read the agreement, here are some key terms you should understand:

- Technology – this includes any ICT systems at the school, including the internet.
- School-owned devices – any devices that are owned by the school that have been made available to you to help with your school work.
- Personal devices – any device that belongs to you that you bring into school, including mobile phones, tablets and laptops.

Security and protecting information

I will:

- Make sure I understand what I can do to keep my information safe when using technology and devices – I will speak to my tutor if I have any questions.

I will not:

- Try to get around any security measures the school has put in place on the internet or school-owned devices.
- Share any of my passwords with other people.

Using technology in school

I will:

- Only use technology and devices that I have been given permission to use.
- Only access websites, apps and other online platforms that I have been given permission to use.
- Only use the school's ICT facilities, technology and devices to complete schoolwork.
- Only go on the internet for something other than schoolwork in my free time.
- Make sure I keep any USB sticks and other removable media safe if they have schoolwork on them.

I will not:

- Install any software onto school ICT systems unless I have been told to do so by a member of school staff.
- Search for, view, download, upload or send anything inappropriate when using the internet.

Emails

I will:

- Only use the email account that has been set up for me by the school when sending emails related to my schoolwork.

I will not:

- Open any emails from people I do not know.
- Use my personal email address for schoolwork, unless I have been told I can do so by a member of school staff.

School-owned devices

I will:

- Only use school-owned devices to carry out my schoolwork.
- Only use websites and apps that a member of staff has said I can use.
- Understand that the school will monitor how I use school-owned devices.
- Take care of school-owned devices when I am using them.
- Tell a member of staff if a school-owned device is damaged or lost when I am using it.
- Tell a member of staff if I think something has happened in relation to the security of the device, e.g. if I download an attachment from an email from someone I do not know.

I will not:

- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to go on personal social media accounts.

Personal devices

I will:

- Leave my phone in my room during lessons and only use it during my free time.
- Only use my other personal devices (e.g. laptop, tablet) during lessons with the permission of the tutor.
- Understand that if my personal devices are lost, damaged or stolen, it is not up to the school to pay for any costs.

I will not:

- Use my personal devices to send inappropriate messages, images, videos or other content.
- Use my personal devices to view, store, download or share any inappropriate, harmful or illegal content.

Social media

I will:

- Think about what I post about the school on social media and make sure I do not post anything that could be harmful to any member of the school community.

I will not:

- Try to speak to any member of staff on social media.

- Accept or send ‘friend’ or ‘follow’ requests from members of staff on social media.
- Send any abusive, threatening or otherwise inappropriate messages on social media.
- Bully anyone through social media.

Artificial Intelligence (AI)

I will

- Use AI tools responsibly following school guidelines.
- Only use AI to support my learning and will follow my school’s rules and teacher’s instructions on when and how to use AI on an assignment.
- Be honest about when I use AI to help with assignments and always reference my sources.
- Review material I source from AI for mistakes and bias.
- Check with my tutor when unsure about what is acceptable.

I will not

- Use AI in a way that could harm myself or others
- Hand in work that is fully created by an AI as my own

Reporting misuse

I will:

- Understand that my use of the internet will be monitored by the ICT technician and recognise the consequences if I do not follow this agreement.
- Understand that the Head of School may decide to take disciplinary action against me, in accordance with the Behaviour Policy, if I do not follow this agreement.

•

Agreement

I agree that I have read and understood this agreement, and ensure that I will abide by each principle.

• **Name**	•
• **Signature**	•
• **Date**	•

Appendix 2

Device and technology acceptable use agreement for staff

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the Head of School in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The school may undertake monitoring activities of employees to ensure the quality and quantity of work. The school will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the school will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as un-intrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. The school understands rights and the private lives of workers, particularly that excessive monitoring can have adverse impacts on data protection rights.

The school will ensure that the monitoring of workers is necessary for the identified reasons. It will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's Data Protection Policy and any other relevant school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Follow the School's E-Safety Policy.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the Head of School or Director of Studies.

- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only access websites and apps that have been approved by the Senior Management Team (SMT).
- Understand that the usage of my school-owned devices will be monitored.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the ICT technician.
- Seek permission from the Head of School before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the Operations Manager.
- Immediately report any security issues, such as downloading a virus, to the ICT technician.
- Make arrangements to return school-owned devices to the Operations Manager upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the Head of School.
- Install any software onto school-owned devices unless instructed to do so by the Head of School or Director of Studies.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices outside of lesson times, i.e. during break and lunch times, or after school finishes at 5:15pm.
- Ensure personal devices are either switched off or set to silent mode during lesson times.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices (including phones) during lessons
- Use personal devices to communicate with pupils or parents.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the Head of School.

Social media and online professionalism

I will:

- Follow the school's guidance on social media in its E-Safety Policy.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:

- Ensure I obtain permission from the Head of School and DPO before any personal data is transferred from a school-owned device to a personal device.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary.
- Ensure my personal device has been assessed for security by the DPO and ICT technician before it is used for home.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

Artificial Intelligence (AI)

I will

- Adhere to the Safe use of AI policy, the E-Safety policy and all other relevant policies.
- Take responsibility for the security of the AI tools and data I use or have access to.
- Model good online behaviours when using AI tools.
- Maintain a professional level of conduct in my use of AI tools.
- Have an awareness of the risks that using AI tools in school poses.
- Report concerns in line with the school's reporting procedure.
- Where relevant to my role, ensure that the safe and appropriate use of AI tools is embedded in the teaching of the curriculum.
- Familiarise myself with any AI tools used by the school and the risks they pose.

I will not

- Use AI in a way that could harm myself or others.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the Head of School.
- Understand that my use of the internet will be monitored by the School and recognise the consequences if I breach the terms of this agreement.
- Understand that the School may decide to take disciplinary action against me, in accordance with the Disciplinary Procedure (In the Employee Handbook), if I breach this agreement.

●

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

● **Name**	●
● **Signature**	●
● **Date**	●