Policy Name	Online Safety Policy				
Effective Date	January 2022	**Date of last revision**	May 2025	**Version No.**	2
Author	Whole School Designated Safeguarding Lead				

Version History				
Version	**Approved by**	**Revision Date**	**Details of Changes**	**Author**
1	**MT/AB**	**30/10/2024**	**Changed name to reflect more modern naming conventions**	**MN**
1	**MT/AB**		**Updated school device and mobile phone section (Bring your own device)**	**MN**
1	**MT/AB**		**Updated all links**	**MN**
2	**AB**	**07.05.2025**	**Addition of Directors/Proprietors to the roles and responsibilities**	**MT**
2	**AB**	**07.05.2025**	**Amendment to the data, to include more recent statistics**	**MT**
2	**AB**	**07.05.2025**	**On Site IT Technician, amended to online**	**MT**
2	**AB**	**07.05.2025**	**Mobile phones to include smart watches and any device with an embedded SIMS**	**MT**
2	**AB**	**07.05.2025**	**Added section on AI in school**	**MT**

Policy Statement

This policy has been developed in conjunction with school stakeholders including:

- Senior Leaders
- Staff
- Parents and carers
- Students

Consultation with the school community has taken place through a range of formal and informal methods – meetings, surveys and focus groups.

The impact of this policy will be monitored using:

- Logs of reported incidents
- Logs of filtering systems
- Surveys of the school community

The aim of this policy is:

- To make clear the various roles and responsibilities of members of the school community
- To provide guidelines for dealing with any online safety incidents

Scope

Under the Education and Inspections Act 2006, the Head of School and Principals are empowered to such an extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying and other online safety incidents covered by this policy, which may take place outside of school but are linked to membership of the school.

The school will deal with such incidents and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place outside of school, as well as those which occur within school grounds and hours.

Definitions of Key Terms

- School community – includes all ICS London staff, students and parents.

The following policies should be read in conjunction with this:

- Data Protection Policy
- Safeguarding Policy
- Behaviour and Anti-Bullying Policy

This policy applies to:

- **Staff**
- **Parents**
- **Students**

Roles and Responsibilities

Directors/Proprietors will:

The Board of directors will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the [Online safety Coordinator, DSL and Senior Leadership Team] are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school

Director with Responsibility for Safeguarding will:

- Approve and review this policy
- Receive reports of serious Online Safety incidents
- Take part in relevant training in order to remain up to date on Online Safety matters.

Head of School and Principal will

- maintain a duty of care for securing the safety of the school community.
- be aware of the procedures to be followed in event of serious online safety allegation being made against a member of staff
- ensure Online Safety Officers receive suitable training to enable them to carry out their roles.
- meet regularly with the Online Safety Officers in order to monitor and support them and receive regular reports on Online Safety within the school.

The Online Safety Officer (Designated Safeguarding Lead) will

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

- provide training and advice for staff
- liaise with school IT technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- meet regularly with Designated Safeguarding Lead who is responsible for all safeguarding investigations including those resulting from the issue of technology
- meet termly with the Head of School
- attends the monthly Whole School Safeguarding meeting

The School is responsible for ensuring

- that the school's technical infrastructure is secure and protected against misuse or malicious attack and limits users.
- that the school meets required online safety technical requirements and any Local Authority / other relevant body guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed where we have set up the Active Directory.
- filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored by the filtering system and that this is done on a school wide basis
- that monitoring software / systems are implemented and updated in accordance with statutory requirements.

Teaching and Support Staff are responsible for ensuring that

- they have an up to date awareness of online safety matters and of the current school IT and Online Safety Policy and practices
- they have read, understood and signed the Staff Code of Conduct which includes the Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Principal /Online Safety Officer for investigation / action / sanction
- all digital communications with students/ parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Members of the Safeguarding Team will

- act as advocates for Online Safety within the School Community
- support the Online Safety Officers with events such as Safer Internet Day
- contribute to reviews of policies and procedures

The Designated Safeguarding Lead will

1. Hold the lead responsibility for online safety, within their safeguarding role.

2. Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.

3. Meet regularly with the Director with Responsibility for Safeguarding responsible for Online Safety at ICS London to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that annual (at least) filtering and monitoring checks are carried out.

4. Attend relevant Board of Proprietors Directors and advisory body meetings.

5. Report regularly to Head of School

6. Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

7. Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

8. be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the

school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through:

- parents' training events, newsletters, letters, the website and information about national and local online safety campaigns.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on:

- the appropriate use of digital and video images taken at school events
- Visitors (volunteers, parents, carers, contractors) may not use mobile phones, cameras, tablets or other devices in the EYFS setting. If parents have children in the setting, they may take pictures of their child(ren) and/or their work only. Any photographs or images that include other children must be deleted.
- Other than in a medical emergency staff, students and visitors are not permitted to use mobile phones or any other mobile / recording devices in areas where students are changing.
- access to parents' sections of the website / ManageBac and on-line student records
- their children's personal devices in the school

Online Safety and the School Curriculum

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The school recognises the breadth of issues involved in keeping children safe online, and that these issues are ever evolving. These issues can be classified in the following ways:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising or phishing

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Students are taught how to stay safe online through our PSHE programme.
- Key online safety messages are reinforced as part of a planned programme of assemblies and within classes.
- Students are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students are helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Staff

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and acceptable use agreements.

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Officer will provide advice/guidance/training to individuals as required.

Social Media

Social media is essential to the lives of young people today as they use it to communicate and keep in touch with friends and family as well as for keeping up to date with the news and current events.

There are many social media platforms used by young people and the Safer Internet Centre Social Media guides resource (available below) should be used to keep up to date with current platforms and their guidelines.

https://www.saferinternet.org.uk/advice-centre/social-media-guides

The almost universal use of social media by young people means it poses a range of risks including but not limited to:

- Cyberbullying
- Online grooming
- Emotional abuse
- Online abuse
- Exposure to harmful images/materials
- Sending or receiving inappropriate images

Educating students on responsible use of social media and the benefits, as well as the risks, falls on all members of the school community. Students are supported through learning about social media in the classroom both during integration into the wider curriculum where appropriate and through stand-alone learning engagements where needed. Opportunities to learn about social media also take place at events for students and families such as learning celebrations/ assemblies/ parent workshops etc.

Incidents on Social Media

Any incident involving an ICS student on social media that is disclosed to a member of staff should be reported to the DSL and recorded on MyConcern. The investigation actions required are the same for any other safeguarding disclosure. The consequences for students in Primary and Secondary school using social media for cyberbullying or bringing the school into disrepute can be found in appendix 6 and 7 respectively.

Exposure to or sending/receiving inappropriate material

- 56% of 11-16 year olds have seen explicit material online
- One-third of British children 12-15 have encountered sexist, racist or discriminatory content
- A third (32%) of 8-17s say they have seen something worrying or nasty online in the past 12 months

(Internetmatters.org, 2021)

- 19% of children, aged 10-15-years-old, exchanged messages with someone online who they never met before in the last year

(https://learning.nspcc.org.uk/online-harm-and-abuse-statistics-briefing.pdf)

With increased use comes increased risk and the above figures demonstrate the likelihood of a student being exposed to inappropriate content online. The school will act proactively to ensure students and their families are clear on the age restrictions in place on various platforms and the reasons behind these.
If a student is exposed to inappropriate content then additional support may be required such as referrals to a counsellor or Westminster Social Services.

Use of Social Media by the school

For learning
Social Media can be a tool used to improve learning engagements. Any use of social media for learning purposes will be referred to the online safety officers in advance of use and permission should be gained from them. The online safety officer may need to request special permissions from the school's IT provider to allow access to a site through the school's firewall.

For marketing purposes
Social media is used by the school for marketing purposes and is managed by the following guidelines:

- Respect parents' and students' (over 12 years old) consent for photo permissions
- Never mention full names, just first names

- Only the marketing coordinator is allowed to post on the school's social media accounts (Facebook, Instagram, Twitter and LinkedIn)
- Never use personal devices to post on the school's social media accounts (refer to Code of Professional Conduct)

Any online communications must not either knowingly or recklessly:

- Place a child or young person at risk of harm, or cause actual harm
- Bring ICS London into disrepute
- Breach confidentiality
- Breach copyright
- Breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
- Use social media to bully another individual or
- Post links to or endorsing material which is discriminatory or offensive

Resources

Safer Internet Centre
NSPCC
Intermatters.org

Acceptable Use

Please see Appendices 1 – 4 for the Acceptable Use Agreements for different parts of the ICS community.

Safe use of digital images and video

When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (eg on social networking sites).

In accordance with guidance from the Information Commissioner's office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites etc., nor should parents/carers comment on any activities involving other students in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Acceptable Use Policy (see Appendices 1, 2 and 3) concerning the sharing, distribution and publication of those images. Images must never be taken using a personal device.

Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or ICS into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

The response to youth produced sexual imagery (sexting) in the form of photographs, video and streaming places children's welfare and protection as a priority and is informed by the Whole School Safeguarding Policy. UK Law states that the making, possessing and distributing of imagery of someone under 18, which is indecent is illegal, including imagery of oneself and is designed to protect young people. Indecent imagery includes imagery of a naked person, a topless girl, an image, which displays genitals, sex acts including masturbation. Indecent imagery may also include overtly sexual imagery of young people in their underwear. In the event of an incident staff must immediately refer to the designated safeguarding lead, who will follow the procedures outlined in the Whole School Safeguarding Policy ensuring that social services and police are notified if there is any concern that a child is at harm. Staff should not view the image and should secure the image where possible and immediately refer to the Principal/ Headteacher. It is illegal for staff to copy, print or share the image.

Written permission from parents or carers will be obtained before photographs of students are published on the school website.

Photographs or video clips published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Student personal information should not be used in any way that makes them easily identifiable e.g. photographs of students will not be named.

Communications

Communication technologies have the potential to enhance learning. Please see Appendix 5 for a table which shows what use of Communication Technologies is permissible in school.

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the Online Safety Officer – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications. Staff should not follow

students on social media or allow themselves to be followed by either current or former students until the student is at least 21 years old.
- Students from Year 3 and above will be provided with individual school email addresses for educational use.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details.
- They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:
- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

School social media accounts should include:
- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:
- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an

appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Dealing with Inappropriate Misuse

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Wherever possible, the opportunity for education and developing student critical thinking in relation to their online behaviour is to be valued.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows.

See Appendices 6 and 7 for Primary and Secondary Consequences respectively.

Dealing with Potentially Illegal Incidents

See Appendix 8: Inappropriate and Illegal Activity Flowchart for procedures for reporting Online Safety incidents.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Where possible conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national/local organisation (as relevant).
  - Police involvement and/or action

- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act (see User Actions chart above)
  - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Infrastructure / Filtering / Monitoring

The school will be responsible for ensuring that the school infrastructure /network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people in the named positions above will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended DfE technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users from PYP3 and above will be provided with a username and secure password and a record will be kept of users and their usernames. Users are responsible for the security of their username and password and will be encouraged to change their password frequently.
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head of School and Bursar and kept in a secure place.

- The remote IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (eg child sexual abuse images) are filtered by the broadband or filtering provider, which actively employs the Internet Watch Foundation CAIC list (Webroot). Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School Online Safety Officers (DSL, Secondary/Primary Principal, Primary) regularly monitor and record the activity of users through Sophos software on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for technical staff to report any actual / potential technical incident / security breach to the Online Safety Officer or Principal.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are reviewed regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed procedure is in place that forbids staff and students from installing programmes on school devices.

Security and Data Protection

ICS takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy for further details.

Any security breaches or attempts, unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Officer

Students and staff have individual school network logins and email addresses. Staff can store files on the school server and google drive. Students and staff are reminded of the need for password security.

All staff and students should

- Use a strong password which should be changed every 6 months
- Not write passwords down
- Not share passwords with other staff or students

Mobile Technologies and School Laptops

ICS London Students are loaned a school laptop on enrolment. This device allows Students to connect to our school network and allows for tight security controls on what applications and settings they can access.

ICS London believes that this enables students to learn better as all students have the same device.

This also allows students to solely connect to the school network and therefore allows the school to consistently filter and monitor web content.

ICS London recognises that Mobile phones can be a useful learning tool, however the school operates a 'no phones' policy by utilising magnetic locking Yondr Pouches. This includes smart watches and any device with an embedded SIMS.

Students are permitted to unlock their pouch and use their phone in lessons with the express permission of their classroom teacher who then assumes responsibility to manage both appropriate use of the mobile phone and ensures that students place their phone back in the Yondr pouch once the lesson has ended.

Staff are prohibited from using their own phones to contact parents. Staff are expected to bring school phones on trips and during off site activities. In an emergency they can contact the emergency services or the school, who will inform the relevant people. Staff may use their own devices for school planning and email.

A wireless SSID is set up across the school sites which is used by students, staff and visitors. Students are given their own individual username and password to access the ICS wireless network. Visitors to ICS (including parents, guest speakers, workmen or parents) are given temporary access via a variety of methods. All wireless traffic at ICS is filtered, then student traffic is routed to avoid ICS servers, routers, printers and databases.

We regularly update the Risk Assessment for bringing in our own devices to reflect changes in recent guidance and internal monitoring. (see Appendix 9).

The use of Artificial Intelligence (AI) systems in school

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. At ICS London we recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and pupils about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and pupils will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and pupils for a future in which AI technology will be an integral part.
- Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR and from the Globeducate group
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum, including supporting pupils to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping pupils with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with

organisational security and oversight requirements, reducing the risk of data breaches.

- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the pupils, being used to train generative AI models without appropriate consent.
- All incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Headmaster, Senior Deputy Head and Designated Safeguarding Lead. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, pupils and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school.
- AI tools may be used to assist teachers in the assessment of pupils' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating to adhere to this agreement, failure to comply will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Responsibilities

The Head of School and the Senior Leadership Team are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Lead / Online Safety Lead

Designated Safeguarding Lead / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer (DPO)

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

IT Manager (Remote)

IT Management will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems. (Schools that have external contracts for technical support must ensure that the support provider is aware of the school's requirements regarding AI and comply with school policies. Such schools should also audit these services for compliance)

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- pupils understand their responsibilities

Proprietors Board of Directors (Governors)

We ensure that our Proprietors Board of Directors (Governors) have a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary.

This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/Carers

We work hard to engage parents and carers by:

- sharing newsletters
- sharing information online e.g., website, social media
- providing curriculum information

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their children's learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

Vulnerable Groups

We recognise that vulnerable pupils are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable pupils are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, pupils and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via: (amend as necessary)

- nominated member of staff

- established school reporting mechanisms
- online/offline reporting tool
- anonymous/confidential reporting routes
- links to national or local organisations

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the pupil at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the Headmaster, Senior Deputy Head and Designated Safeguarding Lead. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems.
- In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk Assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Risk Assessment Matrix

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.	L	H	L	Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.	H	H	M	Monitor AI communication tools, implement clear reporting mechanisms, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.	M	L	L	Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy. Provide appropriate training for all stakeholders.
Emotional Manipulation	AI systems unintentionally affect pupil mental health through curated content.	M	H	M	Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing pupils to harmful or unsuitable materials / behaviour	M	H	M	Conduct rigorous testing of AI tools, apply effective filtering and monitoring and

					ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in pupils	M	H	M	Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact pupil wellbeing or inclusion. AI models produce discriminatory or biased outcomes.	M	M	M	Regularly audit AI algorithms for bias and provide inclusive media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).	M	H	M	Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.	M	M	M	Educate staff and learners to verify AI outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among pupils from diverse demographic groups.	L	M	L	Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and pupils about ethical implications of AI.	L	L	L	Provide training and education on AI ethics and its responsible usage. Establish an ‘Ethics in AI’ group.

Data Accuracy	AI systems generate inaccurate or misleading recommendations.	L	L	L	Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and Pupil data.	L	H	M	Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.	H	H	H	Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and pupils.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.
- Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:
  - PSHRE
  - Cross curricular programmes

- Assemblies, pastoral/tutor time, visits from outside agencies.

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by pupils and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- Pupil assessment
- Critical evaluation of emerging trends and research findings
- Surveys
- Focus groups
- Parental engagement
- Staff consultation
- Engaging with pupils
- Staff training

The following resources are used:

- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (including updated AI reference)
- UKCIS DSIT "Education for a Connected World"

Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Pupils Safe."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.

- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach pupils about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

Appendix 1: Acceptable use Agreement Primary

Responsible Technology Use and Online Safety Agreement
The 3Rs of Technology Use

Student Name: ________________________________

Year Group: __________ **Date:** _________________

It is important to stay safe while using a computer, tablet, phone, or other device and I know that anything I do online may be seen by someone else. The 3Rs must be followed when using technology. I agree to:

Respect Myself by

- Telling my teacher if anything online makes me feel scared or uncomfortable
- Telling my teacher if I get a message that is inappropriate or makes me feel uncomfortable
- Not replying to any unkind or upsetting message which makes me feel upset or uncomfortable
- Always asking my parents first before giving out my mobile number, home number or address to anyone
- Only emailing people from my family and ICS, and asking if I need to email anyone else
- Only using my school email address
- Keeping my password a secret
- Only opening websites which my teacher has said are okay
- Using sites and tools recommended by my teachers and asking if I'm not sure if a site is appropriate for me
- Keeping myself safe by not sharing any personal information (name, address, phone number, where I go to school or hang out, etc.)
- Being principled and not sharing photos of myself or others without asking them and my parents first
- Never agreeing to meet a stranger

Respect Others by

- Making sure all the messages I send are respectful, appropriate and kind

Respect the Environment by

- Taking very good care of ICS technology equipment at all times and following the rules in the device loan charter

If I do not follow the above 3Rs of technology use, my device may be taken from me and I may be suspended from internet use at school. Bullying or any other type of unkind of behaviour online (inside or even outside of school) will still have a serious consequence at school. I understand that my teacher and other adults who work at ICS can monitor my email account and messaging for my own safety and the safety of my classmates.

Student Signature: ____
Date:_________________

PARENTS: PLEASE SEE OTHER SIDE
Parents

□ I have read the above school rules for responsible internet use and agree that my child may have access to IT services via the school IT systems. I understand that the school will take all reasonable precautions to ensure students do not have access to inappropriate websites through our monitoring and filtering software and the vigilance of our teachers, online safety officers, and our IT director, and that the school cannot be held responsible if students do access inappropriate websites.

□ I agree that my child's work can be published on the school website.

□ I agree that during school events, any photos I take will not be published on social media sites if they include other children unless I have individual parent permission for that child

Parent Signature: ____ Date:_________________

Appendix 2: Device Loan Charter - Primary

STUDENT CODE OF CONDUCT FOR DEVICE LOAN CHARTER

Our students will be expected to use the device allocated to them appropriately following the conduct outlined in the Device Loan Charter.

Student name and surname: ________________________________

Parent/Guardian name and surname: ________________________________

Please note: a Device Loan Charter must be provided to the students and signed before the device will be loaned.

Students and parents/guardians must carefully read this charter prior to signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

Device Loan Charter

- I have read the Device Loan Charter.
- I understand my responsibilities regarding the use of the device.
- In signing below, I acknowledge that I understand and agree to the Device Loan Charter and I have also read and understand the Responsible Technology Use Agreement.
- I understand that failure to comply with the Device Loan Charter and/or the Responsible Technology Use Agreement could result in loss of future loan permission for my safety.

Signature of student: ________________________ Date:__________

Signature of parent/guardian: ________________________ Date: _________

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL
For Office use only

Device User Account No: ____________________

Device asset No: ____________________

DEVICE LOAN CHARTER

1. Purpose

The digital device is to be LOANED as a tool to assist student learning both at school and at home.

2. Equipment

2.1 Ownership

2.1.1 The student must bring the device fully charged to school every day if required.

2.1.2 The school retains ownership of the device.

2.1.3 All material on the device is subject to review by school staff. If there is a police request, ICS will provide access to the device and personal network holdings associated with your use of the device.

2.2 Damage or loss of equipment

2.2.1 All devices and batteries are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the device. It does not cover negligence, abuse or malicious damage.

2.2.2 Any problems, vandalism, damage, loss or theft of the device must be reported immediately to the school.

2.2.3 In the case of suspected theft, a police report must be made by the family and an event number provided to the school.

2.2.4 In the case of loss or accidental damage, a parent/guardian should write and sign a statement about how it happened.

2.2.5 Devices that are damaged or lost by neglect, abuse or malicious act, may need to be paid for (up to £400). The Director of ICT will determine whether replacement is appropriate and/or whether or not the student is responsible for repair or replacement costs and whether or not the student retains access to device loans.

2.2.6 Students will be required to replace lost or damaged chargers.

3. Standards for digital device care

The student is responsible for:

- taking care of devices in accordance with school guidelines.
- backing up all data securely. This should be on a memory stick, online storage or on other external storage devices.

- students must be aware that the contents of the devices may be deleted and the storage media formatted in the course of repairs.
- never damaging or disabling digital devices, device systems and networks or establishing, participating in or circulating content that attempts to undermine or bypass device security mechanisms for either software or hardware.

4. Acceptable computer and Internet use

Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

4.1 Access and Security

Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their computer or network account.
- log off at the end of each session to ensure that nobody else can use their computer or network account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Immediately report to the supervising adult (teacher/parent/guardian) if another online user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
  - a message that was sent to them in confidence
  - a computer virus or attachment that is capable of damaging recipients' computers
  - chain letters and hoax emails
  - spam, e.g. unsolicited advertising material.
- never send or publish:
  - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  - sexually explicit or sexually suggestive material or correspondence.

- false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and Internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of ICS.
- ensure that services are not used for unauthorised commercial activities, online gambling or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the Internet or Intranet has the approval of their teacher and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

Students will be aware that:

- they are held responsible for their actions while using Internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.

- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

Students will report:

- any Internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from other schools or other organisations.

ICSLONDON
INTERNATIONAL SCHOOL

Appendix 3: Acceptable use Agreement Secondary

Name: ____
Class: _____________________

This agreement covers the use of computer equipment owned by ICS London and also use of my own device that I bring to school.

I understand that I can use ICS IT systems as long as I behave in a responsible way that keeps me and others safe. I also understand that internet use at ICS is monitored.

I will:

□ only use the school's computers for schoolwork and homework

□ only delete my own files and not access people's files without their permission

□ keep my login and password safe, not let anyone else use it or use other people's login or password

□ not visit websites I know are banned by the school

□ only email people I know or whom my teacher has approved

□ make sure any messages I send or information I upload is polite and respectful

□ not open attachments or download files unless I have permission or I know and trust the person who sent it

□ not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends

□ never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me

□ tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like and I will not respond to any bullying messages

□ only contact ICS staff on the school email system and not try to make any contact with them on any other digital format, including social media and mobile phones

□ only use my mobile phone in school when I have permission

□ not use any internet system to send anonymous or bullying messages

□ log out when I have finished using a school computer

Signed: ____ Date: ______________________

Parents

I have read the above school rules for responsible internet use and agree that my child may have access to ICS IT provision. I understand that the school will take all reasonable precautions to ensure students do not have access to inappropriate websites, and that the school cannot be held responsible if students do access inappropriate websites.

I agree that my child's work can be published on the school website and/or channels authorised by the school.

Signed: ____ Date: ____________________

Appendix 4: Acceptable use Agreement Staff

All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes. Personal use is allowed however this must not bring the school into disrepute or detract from professional responsibilities and personal files must be deleted on demand.

Staff are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken. This applies equally when personal devices are being used within the school environment.

The school reserves the right to monitor internet activity and examine and delete files from the school's system.

Staff have a responsibility to safeguard students in their use of the internet and to report all online-safety concerns to the Online-safety Officer.

Copyright and intellectual property rights in relation to materials used from the internet must be respected.

E-mails and other written communications must be carefully written and polite in tone and nature.

Anonymous messages and the forwarding of chain letters are not permitted.

Staff should not access inappropriate websites or chat rooms.

Communication between staff and students in digital format should exclusively take place through the school email system or other school endorsed channels. Any breach of this rule should be reported to the Online-safety Officer and DSL so as to avoid possible harm to the staff member or student.

Data protection and system security

Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

Files should be saved, stored and deleted in line with the school policy.

Personal use

Staff should not browse, download or send material that could be considered offensive to colleagues and students or is illegal.

Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any hardware used at home safe.

Staff should ensure that personal websites or social media accounts do not contain material that compromises their professional standing or brings the school's name into disrepute.

ICS IT systems should not be used for personal financial gain, gambling, political purposes or advertising.

I have read the above policy and agree to abide by its terms.

Name: ____

Signed: ____
Date: ________________

Appendix 5: Permissible Use of Communications Technologies

	Staff and other adults				Students			
	Not allowed	Allowed	Certain times	Selected staff	Not allowed	Allowed	Certain times	With staff permission
Mobile phones in school		X						X
Use of mobile phones in lessons	X							X
Use of mobile phones in break times		X			X			
Taking photos on personal devices	X							X
Use of school email address for personal emails	X				X			
Use of messaging apps			X		X			
Use of social media			X		X			

Appendix 6: Consequences Matrix Primary

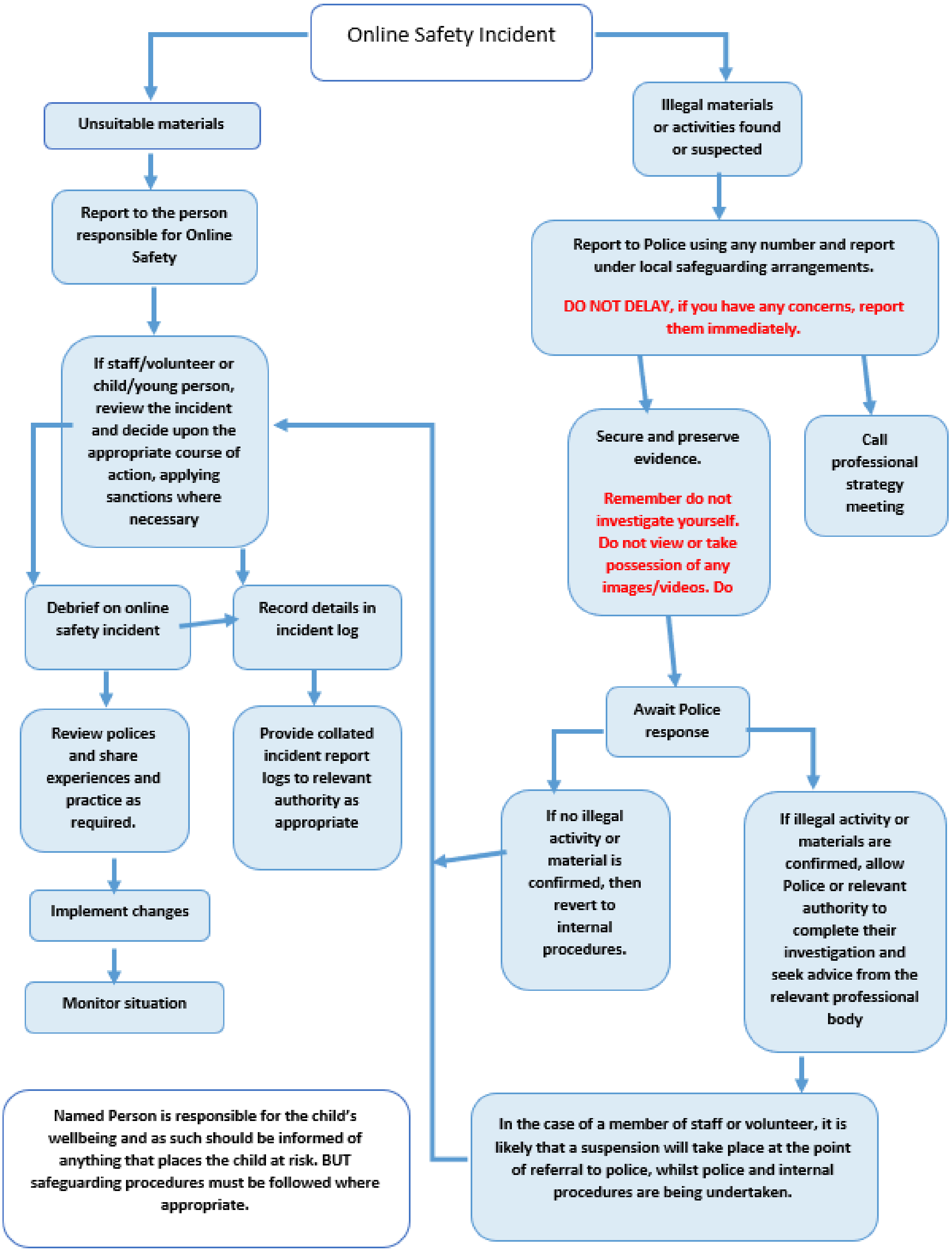
	Class teache r	Online Safety Officer	Parents informed /meeting	Removal of device	Loss of internet access	Principal or Head of School	Suspension / Exclusion	Police
Misuse devices during school time (dependent on nature of misuse)	X	X		X			X	
Repeated misuse of device	X	X	X	X	X	X		
Accidentally accessing material without informing staff	X	X	X					
Cyber-Bullying	X	X	X		X	X		
Deliberately bypassing security / violating privacy of others / destroying data	X	X	X	X	X	X	X	
Persistent / extreme cyberbullying	X	X	X	X	X	X	X	X
Deliberately accessing, distributing offensive* / pornographic material.	X	X	X	X	X	X	X	X
Bringing school into disrepute	X	X	X		X	X	X	

Appendix 7: Consequences Matrix Secondary

	Form Tutor	Online Safety Officer	Parents informed /meeting	Removal of device	Loss of internet access	Principal or Head of School	Suspension / Exclusion	Police
Misuse devices during school time	X	X		X				
Repeated misuse of device	X	X	X	X	X			
Accidentally accessing material without informing staff	X	X						
Cyber-Bullying	X	X	X		X			
Deliberately bypassing security / violating privacy of others / destroying data	X	X	X		X	X	X	
Persistent / extreme cyberbullying	X	X	X			X	X	X
Deliberately accessing, distributing offensive* / pornographic material.	X	X	X			X	X	X
Bringing school into disrepute	X	X	X			X	X	

*Offensive material includes but is not limited to material of a racist, sexist, homophobic, obscene nature.

Appendix 8: Inappropriate and Illegal Activity Flowchart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

References

Keeping children safe in education 2024

Working together to safeguard children 2023

Preventing and tackling bullying, DfE, July 2017

Get safe online

The internet and relationships - ThinkUKnow Guidance

Childnet International

UK Safer Internet Centre - a partner of Childnet International, South West Grid for Learning and the Internet Watch Foundation: co-funded by the European Commission's "Safer Internet Programme"

The South West Grid for Learning - one of the three charity partners of the UK Safer Internet Centre

Child Exploitation and Online Protection Command (CEOPs)

Searching, Screening and Confiscation – Advice for head teachers, school staff and governing bodies 2023

The Counter Terrorism and Securities Act 2015