RIKKYO SCHOOL
ONLINE SAFETY POLICY

Lead Person for Policy: Mr J. Buckles

This policy applies to the whole school

The Policy is available to the school staff via Staff Share

We have a whole school approach to safeguarding, which is the golden thread that runs throughout every aspect of the school. All our school policies support our approach to safeguarding (child protection). Our fundamental priority is our children and their wellbeing; this is first and foremost.

Scope: All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the Policies Register.

Legal Status: Complies with:

- The Education (Independent School Standards) (England) Regulations;
- Keeping Children Safe in Education (KCSIE 2025) DfE: KCSIE 25
- National Minimum Standards (NMS) for Boarding Schools.

Monitoring and Review: These arrangements are subject to continuous monitoring, refinement, and audit by the Headmaster. The Board of Governors will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements, and it will be made available to them in writing or electronically.

Signed:

Date Published: October 2025
Next Review: October 2026

岡野 透	J N Pratten
Dr T Okano	Mr J N Pratten
Headmaster	Chair of GAB

Introduction: The purpose of this Policy is to safeguard students and staff at Rikkyo School. It details the actions and behaviour required from students and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to Online Safety. Our key message to keep students and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our Online Safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding & Child Protection Policy and other related documents.

Online safety is running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding & Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and student Acceptable Use Policies (AUPs) are central to the Online Safety policy should be consulted alongside this policy.

We consider how we can promote online safety whilst developing our curriculum, through our staff training, and through parental engagement. Technology, and risks and harms related to it, evolve, and change rapidly. The Online Safety policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of the experience and changes in legislation or technologies. The Student Council will be consulted regarding any changes to the Student AUP. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important about the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding (Child Protection) Policy, Preventing Extremism and Tackling Radicalisation Policy.

Rikkyo School provides a safe environment for students to learn and work in, especially when online. Filtering and monitoring are both important parts of safeguarding students from potentially harmful and inappropriate online material. The Headmaster has overall strategic responsibility for filtering and monitoring and works in conjunction with the Designated Safeguarding Lead (DSL) and the IT team, as well as the Proprietor to ensure these standards are met. In accordance with KCSIE 2025, the DSL works closely with the members of the Senior Management Team (SMT and the IT team to ensure that filtering and monitoring is adequate and robust in the school and boarding facility. The DSL and IT team:

- procure and maintain an appropriate system (Smoothwall);
- identify risk issue (age of students, Special Education Needs and Disabilities (SEND) issues, English as an Additional Language (EAL), Personal Social Health and Economic Education (PSHEE), Relationship and Sex Education (RSE), County Lines, Bring Your Own Devices (BYOD) etc.);
- carry out regular reviews and
- carry out checks as and when required.
- Ensure that the system is robust and blocks harmful content, without unreasonably affecting teaching and learning.
- Ensure that the chosen system is a member of the Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM). The current system is Smoothwall.

All existing school computers and devices are monitored and checked by the IT lead in association with the DSL and SMT. Boarding students are required to register their e-based devices and are recommended to use the school Wi-Fi system.

Roles and Responsibilities: The DSL has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice in compliance with Keeping Children Safe in Education 2025 (KCSIE 25, DfE), ensuring that effective monitoring strategies are in place that meet the safeguarding needs of the school. The IT Coordinator role overlaps with that of the Online Safety Officer – the DSL, which includes ensuring that:

- students know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep students safe from exploitation or radicalisation.
- students are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- students use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- children, staff, the Governing Body and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement online safety policies and procedures;
- clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting (*no EY in Rikkyo*). Such policies and procedures are to include the personal use of work-related resources.
- the Acceptable Use Policies (AUPs) are to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- monitoring procedures are to be transparent and updated as agreed in School policies.
- allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.

- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- a current record of all staff and students who are granted access to school ICT system is maintained.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL) is a senior member of the management team who has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. The designated persons for safeguarding will be responsible for ensuring that:

- agreed policies and procedures are to be implemented in practice;
- all updates, issues and concerns are to be communicated to all ICT users;
- the importance of online safety in relation to safeguarding is to be understood by all ICT users;
- the training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for;
- working with the UK Board of Governors, IT Lead and other staff, as necessary, to address any online safety issues or incidents; • ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy**;**
- updating and delivering staff training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring;
- liaising with other agencies and/or external services if necessary;
- the learning and development plans of students and young people will address online safety;
- a safe ICT learning environment is to be promoted and maintained.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

The Governing Body's Responsibilities: Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the Governing Body will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement. As part of this process, the Governing Body has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness, and that these standards are discussed with IT staff and service providers to assess what more needs to be done to support the school when appropriate. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified. They consider the number of and age range of the children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

All Staff (including Contractors, Agency Staff and Volunteers): It is the responsibility of all staff to maintain an understanding of this policy, and to be alert to possible harm to students or staff due to inappropriate Internet access or use, both inside and outside of Rikkyo School, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current online safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with Rikkyo School's AntiBullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to the Online Safety Officer which will be placed on staff files. Teachers will ensure they are confident in promoting and delivering online safety as required, implementing this policy consistency, identifying risks and reporting concerns as they arise. All staff are responsible for ensuring that any online safety incidents are logged and dealt with appropriately in accordance with this policy, and ensuring that any instances of cyber-bullying are dealt with in line with the School's behaviour policy.

Parents/Carers: Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately, and ensuring that their child has read, understood and agreed to the terms on acceptable use agreement of the School's IT systems and internet. Rikkyo School will support parents/carers by sharing information and links through newsletters, the school's website, Google Classroom, Microsoft Teams and through formal/informal training. Parents are expected to notify a member of staff or the Headmaster if any concerns or queries regarding this policy. Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-arehttps://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issuesissues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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

All Students: All students will ensure they understand and adhere to our student Acceptable Use Policy, which they must sign and return to the Online Safety Officer. Students are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Breadth of Online Safety Issues: We classify the issues within online safety into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, selfharm, suicide, material against any faith or religion, 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:** personal 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, phishing and or financial scams. If you feel your students, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

These issues are to be managed through the school's filtered Internet, by promoting safe and responsible use, and ensuring both staff and students able to report any concerns to the appropriate people.

Staff/Volunteers Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) (please see appendices) before using any school ICT resource. In addition:

- All staff including the Governing Body will receive appropriate Online Safety training, which is updated regularly;
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other 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.
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the students visit.
- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Any request to do so should be made to the IT Subject Lead.
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved software and email systems which have appropriate security in place.
- Files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes;
- Staff should only communicate electronically with students through the school approved platforms. This includes the school VLE.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities, or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action: •
Report in confidence to the school's member of staff who is responsible for online safety, who is the DSL

- The Online Safety Officer should investigate the incident.
- If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
- In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the Child Exploitation and Online Protection Command (CEOP) and the police will be informed.
- No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and the police will be contacted.

Teaching about Online Safety: Our Online Safety Curriculum is closely linked with our Relationships and Sex Education Programme and discusses the links associated with Online abuse and other associated risks. Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help students to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching students about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Access levels to ICT reflect the curriculum requirements and age of students. Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach including visits from external visitors, an annual E-Safety Week and regular assemblies with a running theme of keeping safe. Students will explicitly be taught the following topics through their lessons:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks;
- How and when to seek support and
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that Peer-on-Peer abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the Internet individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including: • Access to illegal, harmful or inappropriate images;

- Cyber bullying;
- Access to, or loss of, personal information;
- Access to unsuitable online videos or games;
- Loss of personal images;
- Inappropriate communication with others;
- Illegal downloading of files;
- Exposure to explicit or harmful content, e.g. involving radicalisation;
- Plagiarism and copyright infringement;
- Sharing the personal information of others without the individual's consent or knowledge.

Online Safety education is reinforced throughout the year alongside our PSHEE programme, These key message and resources are shared with parents to discuss at home as well. We recognise a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, is used as appropriate. Staff should be vigilant in lessons where students use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy.

Harmful online challenges and online hoaxes: (Please refer to the latest DfE Guidance) There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach students to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern.

Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Students Use of IT Systems: *All students must agree to the IT Acceptable Use Policy before accessing the school systems*. Students will be given supervised access to our computing resources and will be provided with access to filtered Internet and other services operating at the school. Problems with ICT equipment should be reported either to the class teacher or the IT Coordinator. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of students and young people. The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law. Rikkyo School will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre ()
- CEOP's Thinkuknow website
- Teaching Online Safety in School
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff: Staff and the UK Board of Governors will be provided with sufficient online safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the Internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the Internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy/social media policy/user agreement. The Online Safety Officer will act as the first point of contact for staff requiring online safety advice.

Communicating and Educating Parents/Carers in Online Safety: We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of School and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on School website). Parents/carers will also be provided with a copy of the age-relevant Student IT Acceptable Use Policy, and parents/carers will be asked to sign it, as well as the students. Rikkyo School recognises the crucial role that parents/carers play in the protection of their children with regards to online safety. The school organises an annual awareness session for parents/carers with regards to online safety which looks at emerging technologies and the latest ways to safeguard students from inappropriate content.

The school will also provide parents/carers with information through newsletters, and the school VLE, which is FROG. Parents/carers are always welcome to discuss their concerns on online safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents/carers will be encouraged to support the school in promoting good online safety practice.

Acceptable Use of the internet in the School: *All students, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the School's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the School's terms on acceptable use if relevant. Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, proprietors and visitors (where relevant) to ensure they comply with the above.*
More information is set out in the ***acceptable use agreements*** *in appendices 1 and 2.*

Do's and Don'ts <u>DO:</u>

- Talk with your parents about your use of social media and before you open accounts on Facebook and Twitter (X), Instagram, and Snapchat
- Keep your phone on silent or preferably switch it off during lessons
- Consider carefully how you present yourself on Facebook and only refer to your own views and not others' (unless you have their full consent)
- Think carefully about posts that you make and how they may be interpreted. It is important that you do not offend people, use abusive language or discriminate against anyone
- Keep your language civil and polite; do not use profanities when communicating
- Keep details of your personal life and relationships private
- Talk to members of staff if you have concerns about using social networks or if you have a suspicion about a contact
- Report to your parents and/or a member of staff any incident of cyberbullying or intimidation/humiliation
- Make sure you understand how to enable privacy settings. Remember that material posted cannot always be easily removed, so take great care in what you write about yourself and especially others
- Remember that jokes can be misinterpreted or considered offensive and that you must respect the sensitivities of others

<u>DO NOT:</u>

- Give anyone your username or password for the School network
- Play music using MP3 players during lessons or in the corridors
- Play music from your phone or portable device that may annoy or distract others
- Access social media or emails during lessons; this can be done during lunch time and in the dining room
- Try and contact any member of staff by phone, personal email or through social media channels. Staff can contact you via the approved School SMS system or through the designated emails via the School network
- Try and access material or images from extremist groups as these are closely monitored and the School has a legal duty to prevent students from being at risk of radicalisation
- Try and attempt to access inappropriate material, such as pornography, extreme sites or those sites that undermine British values; the School will filter such sites and a monitoring software will be put in place
- Access gaming or gambling sites while at School
- Cut and paste material from the web and claim it as your own work – this is plagiarism, and this is taken very seriously by the School and the examination boards. You can cite, through appropriate referencing, an article or use of quote and staff can guide you in this area. You must respect the law of copyright and intellectual property of others
- Create and display or disseminate offensive material, which includes, but is not limited to, racism, pornography, sexism, bullying (including homophobic bullying), blasphemy, or defamatory material.
- Do not bring the School into disrepute through your communication via emails, your phone, or across social media channels.
- Attempt to "hack" into the network of the School or have any unauthorised access to any part of the network; this is considered a serious breach of our online safety policy.
- Attempt to destroy work files or alter School computer terminals or software in any way.
- Use phones or other portable devices to record (visually or auditory) another student or a member of staff; this will be considered a very serious breach of privacy and will have significant sanction attached to it
- Try and contact teachers or any member of staff through social media; do not ask them to link with you as this is unacceptable and prohibited
- Talk about or discuss members of staff or teachers on your social networks as this could lead to sanctions being taken against you

- Take an image/photograph of another student or member of staff using a smart phone or tablet device unless you have express permission; this is unlikely to be granted by staff for reasons of professional conduct. You must ask friends before tagging them in photos.
- Share any image of a person without their permission
- Impersonate any other person or use another person's account without their full permission
- Post anything that may seem insulting, intimidating, threatening or abusive. The School has a robust anti-cyber bullying policy and this will be enforced if a student is found to have conducted in some form of cyber bullying. Sex-texting will not be tolerated by the School.
- Comment on School policy using social networks - if you need to discuss this, please raise it with the relevant person/appropriate channels. You will been given an opportunity to articulate your comments at a meeting or during the Student Council meetings. (when the School does listen to our students' views on online safety, this is evidenced.)

Sanctions and Enforcement: If a member of the School community breaches any of the terms set out in our policy and guidance documents, sanctions can be applied and in serious cases, any offender will be reported to the appropriate authority. This will be exercised as a case-by-case basis and proportionately. Both staff and students will be subject to disciplinary action depending on the action they have taken and its impact on others, the reputation of the School or in terms of undermining British values.

Cyber Security: The School recognises its responsibility to ensure that appropriate security protection procedures are in place to safeguard are systems. As part of our whole-school Online Safety Training, we ensure staff, the UK Board of Governors and Trustees are updated with the evolving cyber-crime technologies. In addition, the school activity considers the Cyber security standards (DfE: 2023) and uses these as a base for keeping the school and its community safe from cyber-crime**.**

Characteristics of a Strong Password:

- At least 8 characters – the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

Note: do not use < or > in your password, as both can cause problems in web browsers.

A strong password is hard to guess, but it should be easy for you to remember – a password that has to be written down is not strong, no matter how many of the above characteristics are employed.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) 2020. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our online safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will be responsible for ensuring there is an appropriate level of security procedures in place, in order to safeguard systems, staff and learners and will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Additional guidance with regards to information security and access management can be found on the following:

- National Education Network
- Broader guidance on cyber security including considerations for governors and trustees can be found at National Cyber Security Centre - NCSC.GOV.UK.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and promote extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- promoting extreme beliefs;
- accessing likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Rikkyo School has a number of measures in place to help prevent the use of social media for this purpose:

- Website filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by students.
- Students, parents/carers and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation: Rikkyo School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding online safety should be made to the Online Safety Officer, who will review the issue and take the appropriate action. For students, they are taught to raise any concerns to their class teacher who will then pass this on to the Online Safety Officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our Designated Safeguarding Lead (DSL) provides advice and support to other members of staff on protecting students from the risk of online radicalisation. Rikkyo School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of students and know to report any concerns to the DSL.

Assessing Risks: We will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access. Developing technologies, such as mobile phones with Internet access are not governed by the school's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our students, who could have unsupervised access to the Internet when using their own devices. To address this, the school works with students across our age range to ensure that students are educated clearly about the risks of both social media and Internet use, alongside regularly monitoring of device usage as appropriate.

- Mobile phones are not permitted in school (except for year 6 students)
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The UK Board of Governors will review and examine emerging technologies for educational benefit and a risk assessment required by the Prevent Duty will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems except for filtered Wi-Fi access, if necessary.
- Rikkyo School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training. Year 6 students must give any personal mobile devices to the responsible staff member when arriving at school minibus and may collect them on their way back at the end of the day.

Filtering and Monitoring: The school provides a safe environment for students to learn and work in, especially when online. Filtering and monitoring are both important parts of safeguarding students from potentially harmful and inappropriate online material. The proprietor has overall strategic responsibility for filtering and monitoring. For this to occur, they have assigned a member of senior leadership team (The DSL) and the Advisory Board to be responsible for ensuring these standards are met. The DSL works closely with IT lead and other members of SMT to ensure that filtering and monitoring is adequate and robust in the school and boarding facility. The school considers those who are potentially at greater risk of harm and how often they access the school's IT systems. The school follows the Filtering and Monitoring Standards (DfE: 2025) which ensures that the school:

- identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
- reviews filtering and monitoring provision at least annually;
- blocks harmful and inappropriate content without unreasonably impacting teaching and learning (using Smoothwall);
- has effective monitoring strategies in place that meet the school's safeguarding needs.

Phishing and Pharming Definition: A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data. The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity. Pharming is the term used to describe a cyber scam where malicious code redirects a user to a fake website without their knowledge, with the intention of stealing confidential information. As opposed to phishing, pharming requires an attacker to gain unauthorised access to a system. **The school has no intention of changing its financial information, therefore will never accept an email with a link pretending to be the school's accounts department.**

Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S" confirms that the date is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers
- Education on phishing and pharming attacks - staying abreast of phishing scams and the technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist on the Internet that are designed to assist a person in preventing phishing attacks
- Report phishing and pharming to the financial institution, the https://www.gov.uk/report-suspicious-emails-websites-phishing

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; Mobile telephones are not permitted to be used by ANY students during the school day. Year 6 students must give any personal mobile devices to the responsible staff member when arriving at school mini bus and may collect them on their way back at the end of the day. Mobile phones are kept on site at the risk of the individual student. Rikkyo School is not responsible for any devices lost or damaged whilst on School grounds.

Recordings made using mobile electronic devices: Using the camera on a phone or similar device, either to photograph/film/record any member of the School community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

Cyber-Bullying: is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset, intimidate or harass someone else. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. 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 our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to students or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, text messaging etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter (X), Instagram, etc.)** includes the use of defamatory blogs, personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Students should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying**.**

Examining Electronic Devices: School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the School rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Prevent lead or other member of the SMT to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of School discipline), and/or • Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching, and confiscation.
Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the School's complaints procedure.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will be dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and: helpline@saferInternet.org.uk providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
- If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will assess whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT-Based Sexual Abuse (Including Sexting): The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;

- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Sanctions: Sanctions will depend on the severity of the offence as assessed by the Senior Leadership Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the School.
- Temporary or permanent ban on the use of the Internet in the School.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

Chat Room Grooming and Offline Abuse: Our staff need to be continually alerted to any suspicious activity involving computers and the Internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser develops a ‘special’ relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child. Specific focus and attention should be made regarding gaming activities as these are known to be associated with grooming through seemingly innocent contacts.

Social Media, including Facebook, Twitter(X), and Instagram: Facebook, Twitter (X), Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school’s marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Headmaster for reasons of work
- Staff are advised not to befriend or follow parents/carers of students and to keep their personal profile as private as possible
- Staff and students are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and students, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

Staff and students are aware that their online behaviour should always be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy.
Rikkyo School recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Artificial intelligence (AI): Our school recognises that generative artificial intelligence (AI) tools, such as Google Bard and ChatGPT, have many uses. These include enhancing teaching and learning and helping to protect and safeguard students. However, it is crucial that we are aware of the risks carried by AI; for example, facilitating abuse in the form of bullying or grooming, and exposing students to harmful content. This could be in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. It is important that all staff are aware of the risks posed by AI tools, and that risk assessments are carried out for all new AI tools used by our school. Any use of AI to access harmful content or bully students will be treated in line with this policy and our anti-bullying (countering bullying) policy.

Taking and Storing Images of Students Including Mobile Phones Rikkyo School provides an environment in which students, parents/carers and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents/carers, volunteers and visitors are given information (in leaflet form) informing them they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students apart from circumstances as outlined in the Schools Photography and Filming Polic 6 of this policy. This prevents staff from being distracted from their work with students and ensures the safeguarding of students from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy which includes:

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Rikkyo School, taking into consideration staff, students on placement, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that Rikkyo School supports staff, students and parents/carers to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and students respective Behaviour - Code of Conducts. Additionally, Rikkyo School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes the school is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. The School is likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy. Additionally, the Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day-to-day responsibility being delegated to the Online Safety Officer who is our DSL. The Headmaster is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, if it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

For more information relating to Online Safety procedures, refer to the Online Safety Frequently Asked Questions (FAQ) at the end of this document.

5. It covers the following topics on the relevant page as follows:

- How will the policy be introduced to students? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents/carers' support be enlisted?
- Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will students learn to evaluate Internet content?
- How is filtering managed? How are emerging technologies managed? How to react to misuse by students and young people
- How is printing managed? What are the categories of Cyber-Bullying? What are the student rules?
- What has research into Cyber Bullying found? What is the impact on a child of ICT-based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?
- Where can we learn more about Prevent? What do we have to do?
- Do we have to have a separate Prevent Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
- What training must we have? What are the potential legal consequences if we do not take the Prevent duty seriously? What are the rules for publishing content online?

Related documents:

- Online Safety Appendices 1-6
- Safeguarding Children- Child Protection Policy; Sexual Violence and Sexual Harassment (Including Peer-on-Peer Abuse Policy); AntiBullying Policy; Behaviour and Discipline Policy; Staff Behaviour (Code of Conduct) Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy; Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.
- Mobile and Smart Technology Policy, including taking and storing images of students; Acceptable use of ICT Sign off forms for Staff/Students; Use of Photographs Sign-off Form.

Legislation and Guidance for Schools:

You asked for an up-to-date list of the statutory policies and guidance referenced in your online safety policy, each with a current official hyperlink. Below is a comprehensive table, with each entry linking directly to the latest authoritative source. This will help ensure your policy remains current and easily referenceable for staff, governors, and inspectors.

Key Statutory Policies and Guidance for Online Safety (with Hyperlinks)

Policy/Guidance	**Official Link**
Education (Independent School Standards) (England) Regulations 2014	legislation.gov.uk/uksi/2014/3283
Independent School Standards Guidance (DfE)	assets.publishing.service.gov.uk/Independent_School_Standards_Guidance.pdf
Keeping Children Safe in Education (KCSIE) 2025	gov.uk/government/publications/keeping-children-safe-in-education--2
Disqualification under the Childcare Act 2006	gov.uk/government/publications/disqualification-under-the-childcare-act-2006/disqualification-under-the-childcare-act-2006
Working Together to Safeguard Children (2023)	gov.uk/government/publications/working-together-to-safeguard-children--2
Prevent Duty Guidance for England and Wales (2023)	gov.uk/government/publications/prevent-duty-guidance

Policy/Guidance	Official Link
Cyberbullying: Advice for Headteachers and School Staff (DfE)	assets.publishing.service.gov.uk/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Preventing and Tackling Bullying (DfE)	gov.uk/government/publications/preventing-and-tackling-bullying
Data Protection Act 1998	legislation.gov.uk/ukpga/1998/29/contents
UK GDPR and Data Protection Act 2018	gov.uk/data-protection
Teaching Online Safety in School (DfE)	gov.uk/government/publications/teaching-online-safety-in-schools
Education for a Connected World (UKCIS)	https://www.gov.uk/government/publications/education-for-a-connected-world
Harmful Online Challenges and Online Hoaxes (DfE)	https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes
National Curriculum Computing Programmes of Study	https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study
Cyber Security Standards for Schools and Colleges (DfE)	https://www.gov.uk/government/publications/cyber-security-standards-for-schools-and-colleges
Filtering and Monitoring Standards for Schools and Colleges (DfE)	https://www.gov.uk/government/publications/filtering-and-monitoring-standards-for-schools-and-colleges
Human Rights Act 1998	https://www.legislation.gov.uk/ukpga/1998/42/contents
Regulation of Investigatory Powers Act 2000	https://www.legislation.gov.uk/ukpga/2000/23/contents
Computer Misuse Act 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents
Obscene Publications Act 1959	https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
Protection of Children Act 1988	https://www.legislation.gov.uk/ukpga/1988/34/contents
Criminal Justice Act 1988	https://www.legislation.gov.uk/ukpga/1988/33/contents

Note:

- All links are to official government or statutory sources and are current as of November 2025.
- For school-specific or local policies (e.g., Acceptable Use, Anti-Bullying, Behaviour), refer to your school's own policy portal or Rikkyo School's policy page. [Website 学校ポリシーの入れ替え | Outlook]

!

Based on your previous selection, here is a table with the most up-to-date official links for each document:

This Policy also takes into account: Policy/Guidance	Latest Version Link
National Curriculum computing programmes of study	National Curriculum Computing
Meeting digital and technology standards in schools and colleges (DfE: 2023)	Digital and Technology Standards
Filtering and monitoring standards for schools and colleges (DfE: 2023)	Filtering and Monitoring Standards
Cyber security standards for schools and colleges (DfE: 2023)	Cyber Security Standards
Promoting and supporting mental health and wellbeing in schools and colleges (September 2022)	Mental Health and Wellbeing in Schools
Behaviour in schools (September 2022)	Behaviour in Schools Guidance
Guidance (UK Safer Internet Centre)	UK Safer Internet Centre Guidance
2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)	Appropriate Filtering and Monitoring Definitions
Test Your Internet Filter (UKSIC / SWGfL)	Test Your Internet Filter
A Guide for education settings and filtering providers (UKCIS)	Guide for Education Settings and Filtering Providers
Establishing appropriate levels of filtering (UKSIC)	Establishing Appropriate Filtering
Online safety in schools and colleges: questions from the governing board (UKCIS)	Online Safety: Questions from the Governing Board
Sharing nudes and semi-nudes: advice for education settings working with children and young people	Sharing Nudes and Semi-Nudes: Advice

The following legislation and guidance should be considered:

- **Data Protection Act 2018** (which incorporates and supplements the **UK GDPR**) – replaces the Data Protection Act 1998.
- **Human Rights Act 1998** – remains in force, setting out fundamental rights and freedoms under the European Convention on Human Rights.
- **Regulation of Investigatory Powers Act 2000** (as amended) – governs lawful interception, surveillance, and access to communications data; to be read alongside the **Investigatory Powers Act 2016**.
- **Computer Misuse Act 1990** (as amended by the **Police and Justice Act 2006**) – defines criminal offences relating to unauthorised access to or modification of computer systems.
- **Counter-Terrorism and Security Act 2015** – includes the statutory **Prevent duty**, requiring specified authorities (including schools and colleges) to have due regard to preventing people from being drawn into terrorism.
- **Obscene Publications Act 1959** (as amended) – regulates the publication and distribution of obscene material.
- **Protection of Children Act 1978** (not 1988) and **Criminal Justice Act 1988** – provide offences relating to indecent images of children and related safeguarding provisions.

Frequently Asked Questions

Question	Answer
How will the policy be introduced to students?	The policy is introduced through assemblies, lessons, and the Acceptable Use Policy (AUP) which all students must read and sign. Online safety is embedded in the curriculum and reinforced throughout the year.
How will staff be consulted and made aware of this policy?	All staff receive the policy via Staff Share, are required to read and sign the Policies Register, and receive regular training and updates. Updates are communicated in writing or electronically.
How will complaints regarding Internet use be handled?	Complaints are reported to the Online Safety Officer (DSL) and investigated according to school procedures. Serious incidents are escalated to the Headmaster, SMT, or external authorities as appropriate.
How will parents/carers' support be enlisted?	Parents/carers are informed via newsletters, the school website, and annual awareness sessions. They receive copies of the Student AUP and are encouraged to discuss online safety at home and contact the school with concerns.
Why is the use of Internet and ICT important?	Internet and ICT support the curriculum, administration, and professional development, enabling access to educational resources and fostering digital literacy.
How is the safe use of ICT and the Internet promoted?	Safe use is promoted through filtering/monitoring systems, staff and student training, clear AUPs, and regular reinforcement of key messages in lessons and assemblies.
How does the Internet and use of ICT benefit education in our school?	ICT enhances learning, supports research, enables collaboration, and prepares students for the digital world. It is integral to the curriculum and extra-curricular activities.
How will students learn to evaluate Internet content?	Students are taught to critically assess online information, recognise persuasion techniques, and identify risks through lessons and the PSHEE curriculum.
How is filtering managed?	Filtering is managed by the IT team and DSL using Smoothwall, reviewed annually, and blocks harmful/inappropriate content while supporting teaching and learning.
How are emerging technologies managed?	New technologies are risk-assessed before use, and policies are updated as needed. Staff and students receive guidance on safe use.
How to react to misuse by students and young people?	Misuse is reported to the DSL, investigated, and dealt with according to school procedures. Sanctions may include loss of ICT privileges, disciplinary action, or referral to authorities.
How is printing managed?	Printing is monitored to prevent misuse and ensure responsible use of resources. (Note: Specific details may be in the school's ICT or printing policy.)
What are the categories of Cyber-Bullying?	Categories include text message bullying, picture/video-clip bullying, phone call bullying, email bullying, chat room bullying, instant messaging bullying, and bullying via websites/social networks.
What are the student rules?	Students must follow the AUP, use ICT responsibly, not share passwords, not access inappropriate material, and report concerns. Detailed do's and don'ts are listed in the policy.
What has research into Cyber Bullying found?	Research shows cyberbullying can have severe emotional and psychological effects. The policy references the need for vigilance and support for victims.
What is the impact on a child of ICT-based sexual abuse?	ICT-based sexual abuse can cause significant harm, including emotional trauma and risk of further exploitation. The school treats all incidents as safeguarding concerns.
How do I stay secure on the Internet?	Use strong passwords, avoid sharing personal information, be cautious with links/emails, and use secure, school-approved platforms.
Why is promoting safe use of ICT important?	Promoting safe use protects students from harm, supports wellbeing, and ensures compliance with legal and safeguarding duties.

Question	Answer
What does the school's Mobile Phone Policy Include?	Mobile phones are not permitted during the school day (except for Year 6, with restrictions). Use is governed by the Mobile Phone Policy to safeguard students and prevent misuse.
Where can we learn more about Prevent?	Guidance is available in the Prevent Duty policy, DfE resources, and through staff training.
What do we have to do?	Staff must be vigilant, report concerns, follow procedures, and undertake regular training on safeguarding and Prevent.
Do we have to have a separate Prevent Policy?	The school has a Prevent Duty policy, which may be standalone or integrated with safeguarding policies.
What IT filtering systems must we have?	The school uses Smoothwall, which meets DfE filtering and monitoring standards and is reviewed annually.
What is the definition of a visiting speaker?	A visiting speaker is anyone invited to speak to students who is not a regular member of staff.
Do we have to check all our visiting speakers?	Yes, all visiting speakers must be checked and risk-assessed in line with safeguarding procedures.
What checks must we run on visiting speakers?	Identity, suitability, and content of presentations must be checked; records are kept in the Single Central Register.
What do we have to record in our Single Central Register about visiting speakers?	Details of checks, identity, and risk assessments for all visiting speakers.
What training must we have?	Regular safeguarding, online safety, and Prevent training for all staff, updated annually or as needed.
What are the potential legal consequences if we do not take the Prevent duty seriously?	Failure to comply can result in regulatory action, loss of registration, or legal sanctions for the school.
What are the rules for publishing content online?	Content must comply with copyright law, not identify students by full name, and follow school policies on consent and safeguarding.