RUGBY SCHOOL
JAPAN

Online Safety Policy

Version 1.0

Contents

Associated guidance and policies
‘Safeguarding and Child Protection Policy’ Equality Act (2010)
‘Guidelines for Life at Rugby School Japan’
‘Rugby School Japan Complaints Procedure’
‘Rugby School Japan Discipline and Rewards Policy’
‘Rugby School Japan Document Retention Policy’
‘Rugby School Japan Standard Terms and Conditions (Parent Contract)’
‘Rugby School Japan Pupil Manual’

1.0 Associated guidance and policies

1.1 Legislative framework:
This policy has been prepared to meet the School's responsibilities under all relevant legislation, including (but not solely):

Department for Education's guidance on Keeping Children Safe in Education (September 2022)

Department for Education's guidance on National Minimum Standards for Boarding Schools (September 2022)

Department for Education's guidance on Searching, Screening and Confiscation (July 2022)

1.2 Associated RSJ Policies:

Safeguarding and Child Protection Policy

Guidelines for Life at RSJ

Pupil Manual

Discipline and Rewards Policy

Anti-Bullying Policy

Permanent Exclusion and Required Removal Policy

Data Protection Policy

Images Policy

Social Media Policy

Communications Policy

Code of Conduct

Standard Terms and Conditions (Parent Contract)

2.0 Scope of the Policy

2.1 This policy applies to all members of the School community (including governors, staff, pupils, volunteers, parents/guardians, visitors) who have access to and are users of School digital technology systems, both in and out of the School.

2.2 The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils 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 or other online safety incidents covered by this policy, which may take place outside of the School, but is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the School's behaviour policies, including, but not limited to, this policy, the 'Pupil Manual', 'Discipline and Rewards', 'Safeguarding and Child Protection', 'Anti-Bullying', and 'Permanent Exclusion and Required Removal' policies.

2.3 As and when the School becomes aware of any such incidents, it will deal with such incidents in accordance with these policies and will inform parents/guardians.

3.0 Roles and Responsibilities

3.1 The Board

The Board is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. The policy will be approved by the Risk and Compliance Committee. Reviewing the effectiveness of the policy will be carried out by the Pupil Pastoral Welfare Committee. A member of the Board will take on the role of Online Safety Officer. The role of the Online Safety Officer will include:

- annual review of the policy
- regular meetings with the Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to the Full School Board

3.2 Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the School community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator.
- The Principal and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse")
- The Principal is responsible for ensuring that the Online Safety Coordinator, Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal online safety monitoring role.
- The Senior Leadership Team will receive regular updates from the Online Safety Coordinator.

3.3 Online Safety Coordinator

- is the Designated Safeguarding Lead (DSL) or a senior member of staff to whom the DSL has delegated this role (but who reports directly to the DSL for the purposes of the role);
- leads the Online Safety Group;
- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the School online safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provides training and advice for staff;
- liaises with relevant bodies as required;
- liaises with School technical staff;
- receives reports of online safety incidents and maintains a log of incidents to inform future online safety developments;
- meets regularly with the Online Safety Officer to discuss current issues, review incident logs and filtering/change control logs;
- attends the appropriate Governors Sub Committee;
- reports regularly to the Senior Leadership Team.

3.4 IT Director/IT Services Department

Those with technical responsibilities are responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack that the School meets required online safety technical requirements and any other online safety policy/guidance that may apply that users may only access the networks and devices through a properly enforced password protection policy;
- the filtering policy 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in School policies.

3.5 Teaching and O&A Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current School online safety policy and practices;
- they have read, understood and signed the staff Acceptable Use Agreement (AUA);
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation/action/sanction;
- all digital communications with pupils/parents/guardians 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;
- pupils understand and follow the Online Safety Policy and Acceptable Use Agreement;
- pupils 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, pupils 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.

3.6 Designated Safeguarding Lead

Should 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 online contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

3.7 Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the School community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Board. Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production/review/monitoring of the School online safety policy/documents;
- the production/review/monitoring of the School filtering policy and requests for filtering changes;
- reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression;
- monitoring network/internet/filtering/incident logs;
- consulting stakeholders about the online safety provision;
- monitoring identified improvement actions.

3.8 Pupils

- are responsible for using the School digital technology systems in accordance with the pupil acceptable use agreement;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- 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;
- will be expected to know and understand policies on the taking/use of images and on online-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.

3.9 Parents/guardians

Parents/guardians 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, for example:

- Parents' seminars
- Resource provision
- Letters, social media and information about national/local online safety campaigns/literature (e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers)

Parents and guardians 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
- access to the Parent Portal and online pupil records
- their children's personal devices in the School

3.10 Visitors

Visitors to the School who access School IT systems, devices, and infrastructure (including WiFi) will be expected to sign a Visitor User AUA before being provided with access.

4.0 Policy Statements

4.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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 teaching staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of the PSHE programme and should be regularly revisited, with key online safety messages being reinforced as part of this planned programme.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils 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.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside School.
- Staff should 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 pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils 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 IT Services Department can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be addressed to the Online Safety Coordinator and should be auditable, with clear reasons for the need.

4.2 Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be embedded in the annual staff training programme. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out annually.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the School online safety policy and acceptable use policy agreement.
- It is expected that some staff will identify online safety as a training need within the appraisal process.
- The Online Safety Coordinator (or other nominated person) 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 staff as part of ongoing training and feedback will be sought.
- The Online Safety Coordinator (or other nominated person) will provide advice/guidance/training to individuals as required.

4.3 Training – The Board

The Online Safety Officer should receive online safety training, as coordinated by the Online Safety Coordinator.

4.4 Technical – infrastructure/equipment, filtering, and 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 need to ensure that the relevant people named in the above sections 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 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 will have clearly defined access rights to School technical systems and devices.
- All users will be provided with a username and secure password by the IT Services Department, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the School systems, used by the IT Director (or other nominated person), must also be available to the Principal or other nominated senior leader and kept in a secure place.
- The IT Director 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 (child sexual abuse images) is filtered by the broadband or filtering provider..
- Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The School has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the School technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. Breaches/incidents of a safeguarding nature are reported to the DSL via CPOMS. Breaches/incidents of a Technical or Security nature are reported to the IT Department via the Operations Manager
- 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 tested regularly. The School infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School systems.
- Agreed policies are in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on School devices that may be used out of School.
- Agreed policies are in place that forbid staff from downloading executable files and installing programmes on School devices. Downloading of any programme or file which is not specifically related to their job is strictly prohibited and approval from the IT Services Department must be sought to comply with appropriate licensing.
- Agreed policies are in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on School devices. Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

4.5 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be School owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the School's wireless network. The device then has access to the wider internet which may include the School's learning platforms and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a School context is educational. The School acceptable use agreements for staff and pupils give consideration to the use of mobile technologies.

- The School allows:

	School Devices			**Personal Devices**		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in School	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet Only				Yes	Yes	Yes

- The School has provided technical solutions for the safe use of mobile technology for School devices/personal devices:
    - All School devices are controlled through the use of Mobile Device Management software

[1] Authorised device – purchased by the pupil/family through a School-organised scheme. This device may be given full access to the network as if it were owned by the School.

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The School has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this (including the use of VPNs) are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a School location or by an authorised user. These may include: revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling School-licenced software.
- All School devices are subject to routine monitoring.
- Pro-active monitoring has been implemented to monitor activity.
- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.
- Personal devices are brought into the School entirely at the risk of the owner and the decision to bring the device into the School lies with the user (and their parents/guardians) as does the liability for any loss or damage resulting from the use of the device in School.
- The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at School or on activities organised or undertaken by the School (the School recommends insurance is purchased to cover that device whilst out of the home).
- The School accepts no responsibility for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues.
- The School recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the School. Passcodes or PINs should be set on personal devices to aid security.
- The School is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements. In addition:
  - Electronic devices may not be used in tests or exams, unless specifically authorised by the Exams Officer, the Personalised Learning Department or academic staff as appropriate.
  - Users are responsible for keeping their device up-to-date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in School.
  - Confiscation and searching - the School has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended to work is not permitted.
  - The software/apps originally installed by the School must remain on the School owned device in usable condition and be easily accessible at all times. From time to time the School may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
  - The School will ensure that devices contain the necessary apps for School work. Apps added by the School will remain the property of the School and will not be accessible to pupils on authorised devices once they leave the School roll. Any apps bought by the user on their own account will remain theirs.
  - Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
  - Users must only take photographs/share images of people with their permission.

- Devices may be used in lessons in accordance with School protocols.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.

- Pupils may have mobile phones in line with the following rules:
  - Each pupil must provide their mobile phone number to House staff. It is important that the House has a record of all pupil mobile phone numbers for safety reasons.
  - During the School day pupils must avoid the use of mobile phones in public places and around the campus. If pupils are found to be using their phones around the campus, or at times that are not permitted by the guidance below, staff will confiscate them for a period of time and the phone will be kept by the HM until such time as the HM feels the pupil is ready to have the privilege restored.
  - Pupils should only contact staff on their mobile numbers in an emergency situation.
  - The rules regarding access to mobile and other electronic devices are different depending on the year group. Exceptions may be made, by arrangement with the HM, for overseas pupils to phone their parents. The pupils will still have the opportunity to remain in contact with parents and to access social media through their laptops and, should they wish to ring their parents, they will be able to use a House staff phone.

Years 7-9:

Phones may not be used or retained by a Lower School pupil on site until the conclusion of the timetabled School day (defined as 5:30pm during weekdays), except for exceptional purposes and with the permission of the HM/AHM/HA, such as for urgent communication with a family member. A House phone can be made available to boarders for the purpose of contacting family, if needed during the day. Any phones brought to School must be stored with the House staff until 5:30pm on Mondays to Fridays, at which point day pupils will depart for home and boarders will be allowed access to their devices until 6:45pm, when they must be handed back in to House staff for storage. At weekends, all pupils can expect to have their phones returned to them once all School activities have finished on Saturdays (typically at 12:30pm). Boarders remaining in School will be required to hand their devices in on Saturday and Sunday evenings by 9pm. Phones may occasionally be returned to pupils at the discretion of a member of SLT, for example for off-site trips. Boarders must hand in all other electronic devices to House staff overnight.

Years 10-11:

In addition to the access afforded to Year 7-9 pupils, as described above, Middle School pupils (Years 10 and 11) may have access to their phones after the conclusion of prep, and before they should be getting ready for bed (at 9:30pm and 9:45pm respectively). Boarders must hand in all other electronic devices to House staff overnight.

Years 12-13:

Sixth Form (Years 12 and 13) pupils may have their mobile phones at all times of the day. However, they should be switched off in lessons, study lessons and during academic time in the evenings. L6th (Year 12) pupils must hand their phones to House staff at 10pm to be stored until returned on request after 8am the following morning.

4.6 Use of digital and video images

The use of digital and video images is covered by the School's Images Policy.

4.7 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. Details of the School's approach to Data Protection can be found in the School's Data Protection Policy.

5.0 Communications

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

- The official School email service and Google Suite may be regarded as safe and secure. Users should be aware that such communications are monitored. All communications between staff and pupils must therefore be via these methods when in School, or on School Systems (e.g. by remote access) unless permission has been granted by the Deputy Principals to use alternative methods of communication.
- Users must immediately report, to a trusted adult, in accordance with School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature. They must not respond to any such communication.
- Any digital communication between staff and pupils or parents/guardians (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Pupils will be provided with individual School email addresses for educational use.
- Pupils 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.

6.0 Dealing with unsuitable/inappropriate activities

6.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from School and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a School context, either because of the age of the users or the nature of those activities.

6.2 User Actions

The below list gives examples of what would be considered illegal, unacceptable or acceptable at certain times. It is not intended to be an exhaustive list, but as a guide for users of School equipment and systems.

Unacceptable and Illegal:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children.
- Grooming, incitement, arrangement or facilitation of sexual acts against children.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character).
- Criminally racist material – to stir up religious hatred or hatred on the grounds of sexual orientation.
- Promotion of any kind of discrimination
- Promotion of extremism or terrorism

Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to School networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Disabling/Impairing/Disrupting network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

Unacceptable:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- Pornography
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to others or breaches the integrity of the ethos of the School or brings the School into disrepute
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School (for example VPNs)
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- Using School systems to run a private business
- Infringing copyright
- Online gambling
- Online trading (over 18)
- Use of Online Dating apps

Acceptable at certain times:

- Online gaming
- Online shopping/commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting e.g. Youtube & TikTok

7.0 School actions & sanctions

8.1 It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. For pupils this will be in accordance with the Discipline and Rewards Policy. Staff incidents will be dealt with under the Code of Conduct and Discipline Policy and Procedures.

8.2 Examples of pupil incidents are outlined in the below table, along with a possible response. However, each incident will be reviewed on a case-by-case basis and the sanction will be dependent on the seriousness of the offence.

Examples of Pupil Incidents	Issue a Demerit	Issue a School detention	Restriction of technology and network /internet access rights	Further sanction e.g. exclusion
Unauthorised use of non-educational sites during lessons	X			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X			

Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X		
Unauthorised downloading or uploading of files		X	X	
Deliberately accessing or trying to access material that could be considered illegal (see list in “User Actions” section).				X
Deliberately manipulating media to misrepresent a person or their actions				X
Allowing others to access School network by sharing username and passwords			X	X
Attempting to access or accessing the School network, using another pupil's account			X	X
Attempting to access or accessing the School network, using the account of a member of staff			X	X
Corrupting or destroying the data of other users			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			X	X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			X	X
Using proxy sites or other means to subvert the School’s filtering system			X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X

Appendices

Pupil Acceptable Use Agreement
Staff (and Volunteer) Acceptable Use Policy Agreement
Acceptable Use Agreement for Visitors

Pupil - Acceptable Use Agreement

School Policy
Digital technologies have become integral to the lives of children and young people, both within School and outside School. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity and effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that School systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk
- that pupils will have good access to digital technologies to enhance their learning and will, in return, be expected to agree to be responsible users.

Acceptable Use Agreement
I understand that I must use School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will take particular care when disclosing or sharing personal information about myself when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people offline with whom I have communicated online, I will discuss the arrangements with a trusted adult before any meeting takes place.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource:

- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use during lessons or academic time while in School in the evenings.
- I will not try (unless I have permission from the IT Services Department via my HM) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the School systems or devices for online gambling, online dating, file sharing, or video broadcasting (e.g. YouTube and Tik Tok).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the School:

- I will only use my own personal devices (mobile phones/USB devices etc.) in line with the School policy on electronic devices, as outlined in the Online Safety Policy and the Pupil Manual. I understand that, if I do use my own devices in the School, I will follow the rules set out in this agreement, in the same way as if I was using School equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes, software or methods, including VPNs, that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any School device, nor will I try to alter computer settings.
- I will only use social media sites which are accessible through the School network, and never during School activities.
- I shall ensure that any posts which I make are appropriate and do not cause offence.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- I will always cite the work or ideas of others that I use in my own work, in accordance with the School's Academic Integrity Policy.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of School:

- I understand that the School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of School and where they involve my membership of the School community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the School network/internet, temporary or permanent exclusion and, in the event of illegal activities, involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to School systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to School systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the School systems and devices (both in and out of School)
- I use my own devices in School (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the School in a way that is related to me being a member of this School e.g. communicating with other members of the School, accessing School email, VLE, website etc.

Name of Pupil:

Year group:

House:

Signed:

Date:

Staff (and Volunteer) - Acceptable Use Agreement

School Policy
New technologies have become integral to the lives of children and young people, both within School and in their lives outside School. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity and effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The School will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the pupils in the safe use of digital technology and embed online safety in my work with them.

Monitoring
The School regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School will also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School will monitor the contents of a communication (such as the contents of an email).

The purposes of such monitoring and accessing include:

- to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and
- to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.
- Monitoring may be carried out on a random basis, and it may be carried out in response to a specific incident or concern.
- Staff should be mindful that when websites are visited, cookies, tags or other web beacons may enable the site owner to identify and monitor visitors.
- The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of staff visited a blocked website or sent an email containing an inappropriate word or phrase).
- The monitoring is carried out by IT Services. If anything of concern is revealed as a result of such monitoring, then this information may be shared with the Principal and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the police.

For my professional and personal safety:

- I understand that the School will monitor my use of the School digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of School, and to the transfer of personal data (digital or paper based) out of School.
- I understand that the School digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the School. The School permits incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Such use must not interfere with my work commitments or those of others.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I understand that passwords should be long and difficult to guess. I understand that I must not use a password which is used for another account. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I understand that if I leave my workstation or laptop for any period of time, I should take appropriate action to secure information and, in particular, I will lock my screen to prevent access.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Deputy Principal (Pastoral) via CPOMS. If I consider that it may be illegal, I shall contact the DSL immediately.

I will be professional in my communications and actions when using School systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner.
- I understand that any email message or technology-based communication which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, nationality, disability, sexual orientation or religious belief (or otherwise contrary to our Equal Opportunities Policy), or defamatory is not permitted and constitutes gross misconduct.
- I will not include anything in an email or technology-based communication which is not appropriate to be published generally. I understand that anything in an email or technology-based communication may be disclosable under Data Protection disclosures.
- I understand that the School permits incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. I understand that such use must not interfere with my or others' work commitments. I also understand that the School may monitor use of the email section and I should advise those with whom I communicate that this is the case.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the School's Images Policy. I will not use my personal equipment to record these images, unless in accordance with the Images Policy. Where these images are published (e.g. on the School website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites and online platforms in School in accordance with the School's policies.
- I understand that I should only communicate with pupils and parents/guardians using official School systems unless permission has been granted by SLT to use alternative methods of communication. Any such communication will be professional in tone and manner.
- The School permits the use of group communications where necessary, for example the use of email groups or Google groups. I understand that, when using such groups, I should:
    - never share confidential personal details, particularly pupil or parent information;
    - not include parents in the group;
    - be mindful of the School's Online Safety Policy, Images Policy and Code of Conduct;

    - have no expectation that messages sent will remain private, for example the messages may be disclosable under a subject access request or may be used by the School in formal processes if they evidence misconduct or performance concerns.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that emails, texts and other messages are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

The School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the School:

- When I use my mobile devices in School, I will follow the rules set out in this agreement, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses or malware.
- I will not use personal email when conducting School business.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, by using School provided services such as Google Drive, Department areas etc, in accordance with relevant School policies.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes, software or method that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in School policies.
- I will not enter into any contract or subscription on the internet (including through an App) on behalf of the School, without specific permission from the IT Department.
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for School sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of School:

- I understand that this acceptable use policy applies not only to my work and use of School digital technology equipment in School, but also applies to my use of School systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the School.
- I understand that if I fail to comply with this acceptable use policy agreement, I could be subject to disciplinary action in accordance with the School's Discipline Policy and procedure, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the School digital technology systems (both in and out of School) and my own devices (in School and when carrying out communications related to the School) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Visitors - Acceptable Use Agreement

This acceptable use agreement will form part of the sign on procedure to the School systems for visitors.

This acceptable use agreement is intended to ensure:

- that community users of School digital technologies will be responsible users and stay safe while using these systems and devices.
- that School systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use School systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices, and other users. This agreement will also apply to any personal devices that I bring into the School:

- I understand that my use of School systems and devices will be monitored.
- I will not use a personal device that I have brought into School for any activity that would be inappropriate in a School
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files without permission.
- I will ensure that if I take and/or publish images of others I will only do so in accordance with the 'Images' Policy. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the School on any personal website, social networking site or through any other means, unless I have permission from the School.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a School device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the School has the right to remove my access to School systems/devices.
- I understand if I use my device to access inappropriate material or for criminal activity the School will pass on my details to the police.

I have read and understand the above and agree to use the School digital technology systems (both in and out of School) and my own devices (in School and when carrying out communications related to the School) within these guidelines.

Visitor Name:
Signed:
Date:

Date: July 2023