STUDENT ICT AND INTERNET ACCEPTABLE USE POLICY

SLT Lead:	Senior Deputy Head (DP)	**Date Reviewed:**	Lent 24
Circulation:	SLT and Common Room	**Reviewed:**	Lent 25
		Revision / New Policy:	Revision
Ratified by Council:		**Date:**	March 2024

This policy applies to the use of technology on School premises and also any use, whether on or off School premises, which affects the welfare of other students or where the culture or reputation of the School are put at risk.

Rossall School is concerned with establishing a framework of acceptable usage and controls, including student responsibilities, in order to safeguard our ICT hardware, systems, infrastructure and data.

The aims of this policy are to:

- encourage students to make good use of educational opportunities presented by access to the Internet and electronic communication
- to safeguard and promote the welfare of students by preventing "cyberbullying" and other forms of abuse
- minimise the risk of harm to the assets and reputation of the School
- help students take responsibility for their own online safety
- ensure that students use technology safely and securely.
- address the increase in online-related behavioural incidents

Linked Policies

Behaviour Policy
Anti Bullying Policy
Online Safety Policy
Academic Honesty Policy
Safeguarding Policy

Procedures

Students are responsible for their actions, conduct and behaviour online in the same way that they are responsible at all other times. The use of technology should be safe, responsible and legal. Permanent Exclusion is the likely consequence for any student found to be responsible for material on his or her own or another website or social medium or any other electronic material that would be a serious breach of School rules in any other context. Any misuse of the Internet or any electronic media will be dealt with in accordance with the Behaviour Policy.

**Examples of misuse and likely disciplinary action and sanctions are set out in the Appendix. Any misuse should be reported to a member of staff as soon as possible.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups.

Students must not use their own or the School's or any other technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy and Behaviour Policy. If a student thinks that they have been bullied or if another person is being bullied, talk to a member of staff about it as soon as possible. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

If there is a suggestion that a student is at risk of abuse or significant harm, the DSL will deal with the matter under the Child Protection and Safeguarding procedures. If they have reasonable grounds to suspect that possessing that material is illegal, they will report the incident and provide the relevant material to the police as soon as is reasonably practicable.

Using the School's IT systems

Whenever students use the School's IT systems (including by connecting their own devices to the network), they should follow these principles:

- Students should only access School IT systems using their own username and password. Usernames and passwords must not be shared with anyone else.
- Students should not attempt to circumvent the content filters or other security measures installed on the School's IT systems, nor attempt to access parts of the system that they do not have permission to access.
- Students should not attempt to install software on, or otherwise alter, School IT systems.
- Students should not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Students should remember that the School monitors use of the School's IT systems and that the School can view content accessed or sent via its systems.

Email and the Internet

Students are provided with a Rossall School email account to enable them to communicate with other members of the School, primarily their teachers.

When using e-mail the students must ensure that they do not create, access, or pass on material that is obscene, sexually explicit, pornographic, racist, homophobic, defamatory, hateful, bullying, incites or depicts violence or terrorist acts or is otherwise inappropriate or represents values which are contrary to Rossall School’s ethos. All incoming and outgoing electronic data will be monitored for inappropriate content and threats such as computer viruses and other potentially harmful programs.

All Internet activity is monitored and should be used for educational purposes. Attempts to access or download material from obscene, unlawful, violent, abusive or similar sites deemed inappropriate for a School environment will be punishable under the Behaviour Policy.

Students must not use VPNs to circumvent the School's monitoring and filtering systems. Any use of such VPNs without the written consent of the IT Services Manager would constitute a serious disciplinary offence.

Passwords

Students have been issued with a name/password to access resources on the network:

- The password should be changed at the first opportunity (if the system permits)
- Personal passwords should never be shared with friends
- Students have the responsibility to safeguard their passwords and change them regularly to avoid breaches in security and immediately if they suspect they may have been compromised.
- Students are entirely responsible for all activity that occurs using their log-in and must, therefore, safeguard their credentials.

Social media

Inappropriate use of social media, by whatever means, will be dealt with severely, under the terms of the School's Anti-bullying Policy. Such misuse may include, although is not restricted to, impersonating another person online, malicious or defamatory posts or messages and any action which is designed to undermine or defame another member of the School community.

Artificial Intelligence (A.I.)

Submitting work generated by AI/GPT tools as original work is considered a violation of academic integrity and may result in disciplinary action, including but not limited to a failing grade for the assignment or course.

- With permission from a specific teacher in a specific class, students may, on occasion, be permitted to use AI/GPT tools for research, experimentation, and learning purposes, but must clearly distinguish between their own work and any work generated by the tool.
- Any use of AI/GPT tools must be acknowledged in the work and cited appropriately.
- The use of AI/GPT tools is not a substitute for critical thinking, analysis, and originality, which are expected in all academic work.
- Any student found violating this policy will be subject to the disciplinary procedures outlined in Rossall's Academic Honesty Policy.

Youth Produced Sexual Imagery (Sexting)

Students must not send indecent images of themselves, or other students, to another person, whether they are at Rossall School or not. Doing so may constitute a criminal offence. If students commit such an act, it is likely that the local statutory authorities will be consulted and a School disciplinary sanction will be applied. Local statutory authorities include the Police Service and the Lancashire Safeguarding Children Board.

Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them without permission from a teacher during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the School
- Whilst walking around the School site.

Any use of mobile devices in school by pupils must be in line with this Acceptable Use Policy.

No mobile devices should be used to record or photograph another person without their consent. Such incidents are deemed a serious breach of the School rules and may result in permanent exclusion.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may also result in the confiscation of their device.

Monitoring and Filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of pupils and provide them with a safe environment to learn, the School reserves the right to filter and monitor the use of its ICT facilities and network. This includes but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Rossall filters using Sophos, and monitoring using FastVue. This allows for active monitoring of pupils' use. These notifications are dealt with by a member of the Safeguarding team or members of the SLE.

The school monitors ICT use in order to:

- Safeguarding pupils
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the Senior Leadership Executive and the Safeguarding team, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the School's monitoring and filtering systems

The School's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

Search and Delete

Under the Education Act 2011, the Headmaster and any member of staff authorised to do so by the Headmaster, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (your behaviour policy should list these items), **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Safeguarding team.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) or Deputy Head Pastoral of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour Policy
- Involve the DSL (or deputy) or Deputy Head Pastoral without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to DSL and Members of SLE to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Searches and confiscation policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the School complaints procedure.

Unacceptable use of ICT and the Internet outside of school

The School will sanction pupils, in line with the behaviour/discipline policy, if a pupil engages in any of the following **at any time** (even if they are not on School premises):

- Using ICT or the Internet to breach intellectual property rights or copyright
- Using ICT or the Internet to bully or harass someone else, or to promote unlawful discrimination

- Breaching the School's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or live streams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Sharing confidential information about the School, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Retention of Digital Data

Pupils must be aware that all emails sent or received on School systems will be routinely deleted after 3 years and email accounts will generally be closed and the contents deleted within 1 Year of that pupil leaving the School.

Sanctions

Unacceptable use of electronic equipment could lead to confiscation, removal from the School network and other disciplinary sanctions in accordance with the rules set out in this policy, the Behaviour Policy and the Online Safety Policy.

Monitoring and review

The Senior Deputy Head alongside the DSL has responsibility for reviewing this policy and in doing so, will consider any e-safety incidents that have occurred.

Appendix

Senior School & Sixth Form Acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
I will read and follow the rules in the Students ICT and Internet Acceptable Use Policy. **When I use the School's ICT systems (like computers) and get onto the internet in school I will:** ● Always use the School's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my usernames and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I've finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate or which uses the School's brand or logo without prior approval from the School ● Log in to the School's network using someone else's details ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision ● Use AI/GPT in my academic work unless permission is granted and all such work is acknowledged and appropriately cited **If I bring a personal mobile phone or other personal electronic device into school:** ● I will not use it during lessons, tutor group time, when walking around the school site, in clubs or other activities organised by the School, without a teacher's permission ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**
Parent/carer's agreement: When the pupil signs this agreement it is assumed that the parent/carer agrees that the named child can use the School's ICT systems and internet, and, for younger pupils, when appropriately supervised by a member of School staff. Parents agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure the child understands these.

Examples of misuse and disciplinary action and sanctions

The information below is intended to indicate potential sanctions. This is not an exhaustive list.

The SMT reserves the right to adjust these sanctions according to the severity of the misdemeanour.

OFFENCE	POTENTIAL SANCTIONS
Altering the software or hardware configurations of School equipment without authorisation.	First Offence - Saturday detention Escalation - Suspension and final warning
Sharing of inappropriate personal electronic/digital resources, such as pirate movies, pornography etc.	Restriction of account and Inspection and wiping of affected devices. Referral to Deputy Head (Safeguarding and Boarding). Possible action taken under the Child Protection and Safeguarding, Anti-bullying and Behaviour policies.
Attempting to gain access to unsuitable Internet site.	First Offence - After School detention and restriction of device Escalation - Suspension and final warning
Use of abusive, offensive, racist, homophobic, defamatory, aggressive or vulgar language in emails, messaging, online posts or other means of electronic communication.	First Offence - Saturday detention and restriction of device Escalation - Suspension and final warning
Use of webcams or any other device to record still or video images of students or staff without their prior consent.	Will be dealt with under the Anti-bullying and Behaviour policies. Punishments range from a full day Saturday Suspension to Permanent Exclusion.
Impersonation of another person online or an e-mail. The use of another person's social media account.	Sanctions will reflect the severity of the offence and its consequences and may, in extreme cases, include permanent exclusion. If deemed appropriate external agencies may be advised.
Use of a VPN to circumvent system restrictions.	First Offence - Saturday detention and restriction of device Escalation - Suspension and final warning

Intimidation, harassment or bullying by use of emails, text messaging, recorded images or any means of electronic communication.	Students should be aware that depending on circumstances the use of any form of electronic communications to intimidate, degrade or bully any member of the community, could result in suspension, or in extreme cases permanent exclusion.
Bringing the School into disrepute through inappropriate use of electronic media.	Sanctions will reflect the severity of the offence and its consequences and may, in extreme cases, include permanent exclusion.
Using a mobile device around the campus.	First Offence - Demerit and confiscation Escalation - Confiscation and detention issued
Use of AI/GPT without proper acknowledgment / citation	Sanctions will reflect the severity of the offence but may result in the pupil having to repeat the work and a failing grade for the assignment or course.
Production, distribution or sharing of youth produced sexual imagery of any kind.	Statutory services will be consulted and a sanction applied. The severity of the sanction will be decided by the Deputy Head or Headmaster depending on the seriousness of the offence and its effect on others. Sanctions are likely to range from suspension to permanent exclusion. The statutory authorities may also take action against the perpetrators.