RYDAL PENRHOS SCHOOL

Internet & Acceptable Use Policy

INTRODUCTION

Information and Communication Technology (ICT) is an integral part of the way in which Rydal Penrhos School works, and is a critical resource for pupils, staff, Governors, volunteers and visitors. It supports the teaching and learning, as well as the pastoral and administrative functions of the School.

However, the ICT resources and facilities that are used in the School also pose risks to data protection, online safety and safeguarding.

RELATED POLICIES

This policy should be read alongside the School's policies on:

- e-Safety;
- Safeguarding;
- Behaviour, Rewards & Sanctions;
- Staff code of conduct
- Data Protection.

AIMS

This policy aims to:

- set guidelines and rules for the use of School ICT resources for staff, pupils, parents and Governors;
- establish clear expectations as to the way in which all members of the School community engage with each other online;
- support the School's policy on data protection, online safety and safeguarding;
- prevent disruption to the School through the misuse, or attempted misuse, of ICT systems;
- support the School in teaching pupils safe and effective internet and ICT use.

This policy covers all users of the School's ICT facilities, including Governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the staff Disciplinary & Performance Policy & Procedure.

RELEVENT LEGISLATION & GUIDANCE

This policy refers to, and indeed complies with, the following legislation and guidance:

- Data Protection Act (2018);
- The General Data Protection Regulation;
- Computer Misuse Act (1990);
- Human Rights Act (1998);
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000);
- Education Act (2011);
- Freedom of Information Act (2000);
- The Education & Inspections Act (2006);
- Keeping Children Safe in Education (2018);
- Searching, Screening & Confiscation: Advice for Schools (2018).
- Copyright Designs and Patents Act (1988)
- Regulation of Investigatory Powers Act (2000)

DEFINITIONS

ICT Facilities:
This includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, 'phones, music players or hardware, software, websites, web applications or services, and any device, system or service which may become available in the future which is provided as part of the ICT service at the School.

Users:
This comprises anyone authorised by the School to use its ICT facilities, including Governors, staff, pupils, volunteers, contractors and visitors.

Personal Use:
This term covers any use or activity not directly related to the users' employment, study or official purpose.

Authorised personnel:
These are employees authorised by the School to perform systems administration and / or monitoring of the ICT facilities.

Materials:
These are files and data created using the ICT facilities including, but not limited to, documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

UNACCEPTABLE USE

The following is considered an unacceptable use of the School's ICT facilities by any member of the School community. Any breach of this policy may result in disciplinary or behaviour proceedings, as outlined below.

Unacceptable use of the School's ICT facilities includes:

- using the School's ICT facilities to breach intellectual property rights or copyright;
- using the School's ICT facilities to bully or harass someone else, or to promote unlawful discrimination;
- breaching the School's policies and / or procedures;
- any illegal conduct, or 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;
- any activity which defames or disparages the School, or risks bringing the School into disrepute;
- sharing confidential information about the School, its pupils, or other members of the School community;
- connecting any device to the School's ICT network without approval from authorised personnel;
- setting up any software, applications or web services on the School's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
- 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 ICT facilities;
- removing, deleting or disposing of ICT equipment, systems, programs or information without permission from authorised personnel;
- causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- using inappropriate or offensive language;
- promoting a private business, unless that business is directly related to the School;
- using websites or mechanisms to bypass the School's filtering mechanisms.

The above is not an exhaustive list, and the School reserves the right to amend it at any time. The Principal will use his or her professional judgement to determine whether any act or behaviour not on the list above is considered to constitute an unacceptable use of the School's ICT facilities.

Exceptions from unacceptable use:
Where the use of School ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion. Prior approval would be sought via written request to him or her.

Sanctions:
Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the following School policies:

- pupils – Behaviour, Rewards & Sanctions Policy;
- staff – Disciplinary & Performance Policy & Procedure.

STAFF USE

In this context, the term "staff" includes Governors, volunteers and contractors.

Access to School ICT facilities & materials:
The School's IT Services Manager controls access to the School's ICT facilities and materials for School staff. That includes, but is not limited to:

- computers, tablets and other devices;
- access permissions for certain services, programmes or files.

Staff will be provided with unique log-in and / or account information and passwords that they must use when accessing the School's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Services Manager; this can be done via the IT Help desk.

Use of 'phones & email
The School provides each member of staff with an email address which should be used for work purposes only; all work-related business should be conducted using the email address that the School has supplied.

Staff must not share their personal email addresses with parents / carers or pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims of discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act (2018), in exactly the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure, so all email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email; any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible to the intended recipient.

Should a member of staff receive an email in error, then the sender should be informed and the email deleted; should that email contain sensitive or confidential information, the member of staff must not make use of or disclose that information.

If a member of staff should send an email in error which contains the personal information of another person, he or she must inform the IT Services Manager immediately and must follow the School's data breach procedure.

Staff must not give their personal 'phone numbers to parents / carers or pupils, and must use any 'phone provided by the School to conduct all work-related business.

School 'phones must not be used for personal matters, other than those related to work activity as defined in the Mobile 'Phone Policy - Staff; staff who are provided with mobile 'phones as equipment to support their role must abide by the same rules as for ICT acceptable use.

Personal use:
Staff are permitted occasionally to employ School ICT facilities for personal use subject to certain conditions, as set out below. Personal use of ICT facilities must not be overused or abused; the IT Services Manager may withdraw permission for it at any time, or restrict access at his or her discretion.

Personal use is permitted provided that such use:

- does not take place during working hours;
- does not constitute 'unacceptable use';
- takes place when no pupils are present;
- does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the School's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that deployment of the School's ICT facilities for personal use may put personal communications within the scope of the School's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile 'phones or tablets) in line with the School's mobile 'phone policy. They should be aware that personal use of ICT (even when not using School ICT facilities) can have an impact upon their employment by, for instance, putting personal details in the public domain, where pupils and parents / carers could see them.

Staff should take care to follow the School's guidelines on social media (see Appendix 1) and use of email to protect themselves online, and to avoid compromising their professional integrity.

Personal social media accounts:
Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. The School has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

Remote access:
Rydal Penrhos allows staff to access the School's ICT facilities and materials remotely; this is supervised by the IT Services Manager and can be requested via the IT Help Desk.

Staff accessing the School's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site; staff must be particularly vigilant if they use the School's ICT facilities outside the School premises, and must take such precautions as the IT Services Manager may require from time to time against importing viruses or compromising system security.

The School's ICT facilities contain information which is confidential and / or subject to data protection legislation; such information must be treated with extreme care and in accordance with our data protection policy.

School social media accounts:
The School has official Facebook and Twitter pages which are supervised by the Communications Manager. Staff members who have not been authorised to manage, or post to, this account must not access or attempt to access the account.

The School has guidelines as to what can and cannot be posted on its social media accounts; those who are authorised to manage the account must ensure that they abide by these guidelines at all times.

The monitoring of the School network and the use of ICT facilities:
The School reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, the monitoring of:

- internet sites visited;
- bandwidth usage;
- email accounts;
- telephone calls;
- user activity and / or access logs;
- any other electronic communications.

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- 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.

PUPIL USE

Access to ICT facilities:
Computers and equipment in the School's ICT suites are available to pupils only under the supervision of staff. Specialist ICT equipment, such as that used for Music or Design & Technology, must only be used under the supervision of staff.

Sixth Form pupils can use the computers in the Ferguson Centre independently, but for educational purposes only.

Search & deletion:
Under the Education Act (2011), and in line with the Department for Education's Guidance on Searching, Screening and Confiscation, the School has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under School rules or under legislation.

The School can, and will, delete files and data found on searched devices if it is believed that the data or file has been, or could be, used to disrupt teaching or to break the School's rules.

The unacceptable use of ICT and the Internet outside School:
In line with the Behaviour, Rewards & Sanctions Policy, the School will sanction a pupil if he or she engages in any of the following activities at any time, even if he or she not on School premises at the time:

- 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 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;
- 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 ICT facilities or materials;
- causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- using inappropriate or offensive language.

PARENT / CARER USE

Access to ICT facilities & materials
Parents / carers do not have access to the School's ICT facilities as a matter of course. However, parents / carers working for, or with, the School in an official capacity (for instance, as a volunteer or as a member of the Friends of Rydal Penrhos School) may be granted an appropriate level of access, or may be permitted to use the School's facilities at the Principal's discretion. Where parents / carers are granted access in this way, they must abide by this policy in the same way as it applies to staff.

Communicating with or about the School online:
Rydal Penrhos believes that it is important to provide a model for pupils, and to help them to learn how to communicate respectfully with, and about, others in the online context. Parents / carers play a vital role in helping to model this behaviour for their children, especially when communicating with the School through its website and social media channels.

Rydal Penrhos asks parents / carers to sign the agreement at Appendix 2.

DATA SECURITY

The School takes measures to protect the security of its computing resources, data and user accounts; however, it cannot guarantee security. Staff, pupils, parents / carers and others who use the School's ICT facilities should use safe computing practices at all times.

Passwords:
All users of the School's ICT facilities should set strong passwords for their accounts and should keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files that they control. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents / carers or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls & anti-virus software:
All of the School's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards that the School implements and maintains so as to protect personal data and the School's ICT facilities.

Any personal device using the School's network must be configured in this way.

Data protection:
All personal data must be processed and stored in line with data protection regulations and the School's Data Protection Policy.

Access to facilities and to materials:
All users of the School's ICT facilities will have clearly defined access rights to School systems, files and devices; these access rights are controlled by the IT Services Manager.

Users should not access, nor should they attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something to which a user should not have access is shared with them, they should alert the IT Services Manager immediately.

Users should always log out of systems and should lock their equipment when it is not in use in order to avoid any unauthorised access. Equipment and systems should always be logged out of at the end of each working day.

Encryption:
The School ensures that its devices and systems have an appropriate level of encryption. School staff may only use personal devices (including computers and USB drives) to access School data, to work remotely, or to take personal data (such as pupil information) out of School if they have been specifically authorised to do so by the Principal.

The use of such personal devices will only be authorised if these devices have appropriate levels of security and encryption, as defined by the IT Services Manager.

INTERNET ACCESS

The school provides access to the internet via wired and wireless networks which are secured by various means; this includes separate wireless networks for staff, pupils and guests. All access to the internet is filtered and monitored such that any breach detected by the filtering system will generate alerts to the IT Services Manager. Occasionally the filtering system may categorise sites in error - if this is the case, users must report it to the IT Services Manager immediately.

Pupils:
Wi-Fi is widely available throughout the School campus; however, it is only accessible during certain hours in boarding houses. Various filtering policies are currently applied to ensure that pupils can only access age-appropriate content, and this includes limiting access to social media, instant messaging, gaming sites and services.

If a pupil needs access for educational purposes, they can request this via the IT Services Manager.

Parents & visitors:
Parents and visitors to Rydal Penrhos will not be permitted to use the School's Wi-Fi unless specific authorisation is granted by the Principal, and this will only be forthcoming under the following circumstances:

- parents are working with the School in an official capacity (e.g. as a volunteer);
- visitors need to access the School's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

Staff must not give the Wi-Fi password to anyone who is not authorised to have it; doing so could result in disciplinary action.

MONITORING & REVIEW

The Principal and the IT Services Manager monitor the implementation of this policy and will ensure that it is updated to reflect the developing needs and circumstances of the School.

This policy is subject to review on a biennial basis; however, it may require earlier revision in the light of any regulatory change which may come into force in the interim.

Adopted (SLT):	February 2022
Review dtae:	February 2024

APPENDIX 1: FACEBOOK 'CHEAT SHEET' FOR STAFF

Do not accept friend requests from pupils on social media

TEN RULES FOR SCHOOL STAFF ON FACEBOOK:

- change your display name – use your first and middle name, use a maiden name (if married) or put your surname backwards instead;
- change your profile picture to something unidentifiable or, if not, ensure that the image is professional;
- check your privacy settings regularly;
- be careful about tagging other staff members in images or posts;
- do not share anything publicly that you would not be just as happy showing to your pupils;
- do not use social media sites during School hours;
- do not make comments about your job, your colleagues, the School or its pupils online – once it is out there, it is out there;
- do not associate yourself with the School on your profile (e.g. by setting it as your workplace, or by 'checking in' at a School event);
- do not link your work email address to your social media accounts. Anyone who has this address (or your personal email address / mobile 'phone number) is able to find you using this information;
- consider uninstalling the Facebook app from your 'phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents / carers or pupils).

CHECK YOUR PRIVACY SETTINGS

- change the visibility of your posts and photos to **'Friends only'**, rather than to 'Friends of friends'; otherwise, pupils and their families may still be able to read your posts, see things you have shared and look at your pictures if they are friends with anybody on your contacts list;
- do not forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts;
- do not forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts;
- the public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster;
- **Google your name** to see what information about you is visible to the public;
- prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this;
- remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

WHAT TO DO IF A PUPIL ADDS YOU ON SOCIAL MEDIA

- in the first instance, ignore and delete the request. Block the pupil from viewing your profile;
- check your privacy settings again, and consider changing your display name or profile picture;
- if the pupil asks you about the friend request in person, tell him or her that you are not allowed to accept friend requests from pupils and that, if they persist, you will have to notify Senior Leadership and / or their parents / carers. If the pupil persists, take a screenshot of his or her request and any accompanying messages;
- notify the Senior Leadership Team or the IT Services Manager about what is happening.

WHAT TO DO IF A PARENT / CARER ADDS YOU ON SOCIAL MEDIA

- it is at your discretion whether to respond. Bear in mind that:
    - responding to one parent's / carer's friend request or message might set an unwelcome precedent for both you and other teachers at the School;
    - pupils may then have indirect access through their parent's / carer's account to anything you post, share, comment on or are tagged in;
- if you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent / carer know that you are doing so.

WHAT TO DO IF YOU ARE BEING HARASSED ON SOCIAL MEDIA, OR IF SOMEONE IS SPREADING SOMETHING OFFENSIVE ABOUT YOU

- **do not** retaliate or respond in any way;
- save evidence of any abuse by taking screenshots and recording the time and date it occurred;
- report the material to Facebook or the relevant social network and ask them to remove it;
- if the perpetrator is a current pupil or staff member, the School's mediation and disciplinary procedures are usually sufficient to deal with online incidents;
- if the perpetrator is a parent / carer or other external adult, a senior member of staff should invite him or her to a meeting to address any reasonable concerns or complaints and / or request that he or she remove the offending comments or material;
- if the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

APPENDIX 2: ACCEPTABLE USE OF THE INTERNET – AGREEMENT FOR PARENTS / CARERS

Acceptable use of the internet: agreement for parents / carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents / carers to communicate with, or about, the School. The School uses the following channels: • the official Facebook page; • email / text groups for parents / carers (for School announcements and information); • the School's virtual learning platform. Parents / carers also set up independent channels to help them stay up-to-date with what is happening in their child's class. For example, class / year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the School via official communication channels, or using private / independent channels to talk about the School, I will: • be respectful towards members of staff, and the School, at all times; • be respectful of other parents / carers and children; • direct any complaints or concerns through the School's official channels, so they can be dealt with in line with the School's complaints procedure. I will not: • use private groups, the School's Facebook page or personal social media to complain about or criticise members of staff. This is not constructive and the School cannot address or resolve issues if they are not raised in an appropriate way; • use private groups, the School's Facebook page or personal social media to complain about, or to try to resolve, a behaviour issue involving other pupils. I will contact the School and speak to the appropriate member of staff if I am aware of a specific behaviour issue or incident; • upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents / carers.	
Signed:	**Date:**

APPENDIX 3: ACCEPTABLE USE AGREEMENT FOR OLDER PUPILS

Acceptable use of the School's ICT facilities and internet: agreement for older pupils & parents / carers	
Name of pupil:	
When using the School's ICT facilities and accessing the internet in School, I will not: • use them for a non-educational purpose; • use them without a teacher being present, or without a teacher's permission; • use them to break School rules; • access any inappropriate websites; • access social networking sites (unless my teacher has expressly allowed this as part of a learning activity); • use chat rooms; • 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; • share my password with others or log in to the school's network using someone else's details; • bully other people. I understand that the School will monitor the websites I visit and my use of the School's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the School's ICT systems and internet access responsibly. I understand that the School can discipline me if I do certain unacceptable things online, even if I am not in School when I do them.	
Signed (pupil):	**Date:**
Parent / carer agreement: I agree that my child can use the School's ICT systems and internet access when appropriately supervised by a member of School staff. I 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 that my child understands these.	
Signed (parent / carer):	**Date:**

APPENDIX 4: ACCEPTABLE USE AGREEMENT FOR YOUNGER PUPILS

Acceptable use of the School's ICT facilities and internet: agreement for younger pupils and parents / carers	
Name of pupil:	
When I use the School's ICT facilities (such as computers and equipment) and get on the internet in School, I will not: • use them without asking a teacher first, or without a teacher in the room with me; • use them to break School rules; • go on any inappropriate websites; • go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson); • use chat rooms; • open any attachments in emails, or click any links in emails, without checking with a teacher first; • use mean or rude language when talking to other people online or in emails; • share my password with others or log in using someone else's name or password; • bully other people. I understand that the School will check the websites I visit and how I use the School's computers and equipment; this is so that they can help keep me safe and make sure I am following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a School computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the School's ICT systems and internet. I understand that the School can discipline me if I do certain unacceptable things online, even if I am not in School when I do them.	
Signed (pupil):	**Date:**
Parent / carer agreement: I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I 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 that my child understands these.	
Signed (parent / carer):	**Date:**

APPENDIX 5: ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS & VISITORS

Acceptable use of the School's ICT facilities and the internet: agreement for staff, Governors, volunteers and visitors	
Name of staff member / Governor / volunteer / visitor:	
When using the School's ICT facilities and accessing the internet in School, or outside School on a work device, I will not: • access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material); • use them in any way which could harm the School's reputation; • access social networking sites or chat rooms; • use any improper language when communicating online, including in emails or other messaging services; • install any unauthorised software, or connect unauthorised hardware or devices to the School's network; • share my password with others or log in to the School's network using someone else's details; • share confidential information about the School, its pupils or staff, or other members of the community; • access, modify or share data that I am not authorised to access, modify or share; • promote private businesses, unless that business is directly related to the School.	
I understand that the School will monitor the websites I visit and my use of the School's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside School, and will keep all data securely stored in accordance with this policy and the School's data protection policy. I will let the Designated Safeguarding Lead and IT Services Manager know if a pupil informs me that he or she has found any material which might upset, distress or harm him, her or others, and will also do so if I encounter any such material. I will always use the School's ICT systems and internet responsibly, and will ensure that pupils in my care do so too.	
Signed (staff member / Governor / volunteer / visitor):	**Date:**