REDRUTH SCHOOL

Acceptable Use Policy

This policy was adopted February 2017

This policy is to be reviewed annually

The designated individual is Mr Adrian Hill

Use of the school network is for educational purposes only

ICT Staff Acceptable Use Policy

Definitions used in this policy:

The School - Redruth School.
School Network - computers joined together to allow users to share hardware, software and data. The school network includes cable and wireless media and online access to the Internet.
School ICT hardware - equipment bought, hired, licensed or otherwise obtained by the school for authorised users and uses authorised.
School ICT software - software bought, hired, licensed or otherwise obtained by the school for authorised users and uses authorised by the school.
Email - sending of text messages and/or computer files from user to user over a communications network.
The Internet - a collection of interconnected computer networks around the world.
User account - a unique record on the school network that describes an individual user's limited access to the school network. The user account is password protected.
User ID - the name given to an individual user account.
StAUP - the policy set out in this document, known as 'The Redruth School Staff Acceptable Use Policy'.

The Purpose of this policy

This policy sets out the rationale for users' limited access to the school network, ICT hardware and software. It applies to all users and administrators of Redruth School's network. It describes the services offered to staff and sets out what are acceptable uses. It stands alongside other school rules and regulations, contractual terms and conditions of employment. Nothing in this policy will replace or override any other rules and regulations, contractual terms and conditions of employment.

Disclaimer

Users accessing the school network, Internet and email do so at their own risk and although the school network is carefully managed to minimise risk, Redruth School cannot accept any liability for any hardware, software or data lost or damaged, including coursework.

The School is not responsible for material viewed or downloaded by users from the Internet. To minimise these risks, use of the Internet at Redruth School is governed by the StAUP.

1. Limited use of the school network, Internet and email

1.1 The school encourages all users to make effective use of the school network, Internet and email. Such use must always be lawful. It must not compromise the School's information and computer systems/networks.

1.2 The users shall ensure that the use of the Internet and email will not adversely affect the school or its business, in particular damage the school or its employees' reputations or otherwise violate any of the schools policies.

2. The Use of the network and Internet at Redruth School

2.1 Subject areas will provide:

- Opportunities to develop a broad range of ICT skills and capabilities that will facilitate learning and develop understanding of the role of ICT in the modern world;
- Skills, knowledge and attitudes which allow users to judge critically and effectively the validity and safety of information they find on the Internet;
- Explicit opportunities to discuss moral and ethical issues associated with the use of the Internet.
- The use of the network/internet must comply with the E-Safety Policy (Oct 2013)
- Mobile devices will only be allowed to be use on the school network/internet connection with the approval of the Redruth School Senior leadership Team. Devices will be controlled and monitored by RM SafetyNet and Impero.

- 2.2 Use of the Internet should:
- Enhance students' learning opportunities and outcomes in key learning areas;
- Assist students and staff to develop the information and communication skills necessary to use the Internet effectively and appropriately;
- Reflect community values.

3. Responsibilities of Staff Members

3.1 Staff members in Redruth School will use the school network, Internet and email for instructional purposes and will accept the Acceptable Use Policy electronically, details of which will be stored centrally.

3.2 Staff members should maintain the highest ethical behaviour in using the school network, Internet and email and should promote that behaviour among students. Staff members will:

- Make use of the school network for curricular purposes only and make every attempt to maintain the curricular focus of school network, Internet and email use by locating and directing students towards worthwhile sites on the Internet and appropriate use of email;
- Supervise student use;
- Ensure that all students are aware of E Safety when using the school network and internet.
- Model and provide instruction in the ethical and appropriate use of the school network, Internet and email in a proper school setting as provided in the following guidelines;
- Strive to ensure that Internet resources are appropriate to the individual student's instructional needs, learning styles, abilities and developmental level.
- Accept that communications via the Internet and email are not normally secure or encrypted and staff should therefore take particular care when sending potentially sensitive or confidential information.
- Strive to ensure that their work is in line with the Data Protection Act at all times.
- Not use the network for viewing, saving or sending any inappropriate data which would/could be seen to be offensive and bring the school in to disrepute.
  - Have photographs of students in their personal user area
  - Not use social media sites to communicate with students, unless it is essential for educational purposes for which authority must be gained from the Headteacher
  - Only use the default screensaver and all other changes should be authorised by the Network Manager.
  - Not use school email for personal use.

- Laptops should be connected to the school network on a regular basis to perform security updates.
- Staff must not allow students network access using staff logins details at any time.
- Staff should actively maintain their user area and network drives G and K and should ensure that files are stored appropriately within the schools folder structure e.g. deleting out of date files including photographs.
- Staff must notify the Network Manager before installing, or arrange installations of, software applications on any Network device (Servers, Laptops, Desktops, Ipads or any school mobile device)
- Staff must notify the Network Manager of any BYOD requiring access to the school wireless network
- Personal data, videos, photos etc must not be stored on the network.
- Itunes etc must not be installed on any computer and used to backup data from personal phones, Ipads etc without the Network Manager being notified.

4. Management of Remote Access

4.1 Remote Access for Staff is managed by the Network Manager/Assistant Network Manager.

- Remote Access allows Staff to access data in their user area (N drive), shared areas drives K,G,T and SIMS.
- Remote access for staff is controlled through Group Policy membership. Group Policy membership will only be granted to members of staff agreed by the Headteacher.
- Group Policy membership may be granted on an ad-hoc basis.
- Inactive Remote Access session timeouts will be set to 5 minutes.
- Remote Access sessions will automatically terminate after one hour.
- Remote access sessions must not be left unattended under any circumstances. Sessions must be terminated immediately.
- Screen savers must be setup on home device used for Remote Access.

5. Management of User Access

5.1 Access to all school systems is via user accounts which require successful authentication using a password.

5.2 Where a user requires access to resources beyond their user account, this may be arranged by the Network Manager, as appropriate. Requests to be submitted via 'help desk (online call logging service)'.

5.3 Ensure that Staff User ID’s use a **strong password** consisting of at least eight characters (the more characters, the stronger the **password**) that are a combination of letters (upper and lower case), numbers and symbols.

Users must not divulge their passwords or user ID's to anyone and must keep them confidential and secure. Password changes will be forced on a regular basis.

Different passwords should be used for network and SIMS logins.

5.4 Users accept that communications sent via the School's email system may be monitored for the purpose of ensuring appropriate use of the system. Users should also be aware that deleted emails and files may still be accessible via back-up systems

5.5 Users need to be aware that personal details may also be stored on the School's network servers or local devices and must accept the associated risks. At regular intervals a random selection of user areas and devices will be audited to ensure compliance with the Computer Misuse Act (1990) and the Data Protection Act (2003) as well as the school's Acceptable Use Policy.

5.6 Modem access from the school's network to public networks is not permitted, without prior authorisation from the Headteacher, as this method by-passes the school's security equipment.

5.7 Users of laptops and other forms of mobile computers should protect any sensitive information copied onto a local system by password. Highly sensitive information must be protected by disk encryption. Data stored on user's laptops should be backed up to memory sticks or network. Any sensitive school data saved on mobile devices must be stored on encrypted media (Memory Sticks, Laptops and Portable Hard-Drives) especially if going off site.

5.8 Users of mobile technologies should avoid risk of eavesdropping by using the equipment in a suitable location. These items of equipment should be suitably stored to reduce the risk of vandalism or theft.

5.9 Leavers are advised that files held on computer systems and their email accounts will be accessed after their employment terminates so that any files and emails can be re-allocated. Their user access rights will be removed after 2 weeks and user accounts suspended and subsequently deleted.

5.10 Laptops are setup for school use, ICT Support are not responsible for configuration of Broadband connectivity off site.

5.11 The Network Manager must be informed immediately of any virus on any school equipment.

6. The Responsibilities of the School

6.1 The School undertakes a commitment to provide appropriate physical and financial resources to facilitate the successful incorporation of access to on-line and networked services throughout the curriculum.

6.2 The School will actively support the professional development of all staff to ensure the effective inclusion of information technologies, including the relevant information skills, into the School curriculum.

6.3 The school shall report, to the appropriate authorities, all known incidents of Internet and email violation that contain or breach the following:

- Images of child pornography or child abuse;
- Adult material/pornography that potentially breaches the Obscene Publications Act (1959 and 1964);

- Criminally racist material;
- Computer Misuse Act (1990);
- Telecommunications Act (1997).
- Data Protection Act (2003)
- Inappropriate social networking activity

6.4 The school will seek to protect individuals' privacy and safety

- The School will not provide identifying data, such as full name, address or other information, which describes the personal situation or location of students, staff or community members.
- The School will only publish images of students on the Internet in line with the School's Use of Images of Children consent form.
- Users should not provide personal information about themselves or others across the Internet. It is very difficult to ensure that people are who they claim to be.
- The School will provide removable media encryption devices/software where necessary. This will maintain a high level of security to sensitive data being taken off the school network.

7. Code of Behaviour

7.1 Staff must read and accept the Acceptable Use Policy Undertaking before access to any computer system or the Internet and email is permitted.

7.2 Breaches of the Acceptable Use Policy, and/or other Rules, Responsibilities and Procedures related to the Internet and email will result in disciplinary action in line with current procedures. In addition law enforcement agencies may be involved, if deemed appropriate.

Cross References: Child Protection
Images
Disciplinary