BYRCHALL HIGH SCHOOL

Makerfield Community Trust

E-Safety Policy

(Revised June 2014)

Please read this policy carefully as you will, in future, be deemed to be aware of its contents in the event that there is any breach of the terms described in this document

Terminology

From here on, the terms listed below will be defined as follows:

a) The School – Byrchall High School.

b) User(s) – Any person(s) who is granted permission to use, within the bounds of this and other applicable ICT policies, any aspect of the computer resources provided by Byrchall High School. Typically this covers all staff, students and parents or carers of students, but will also extend to other stakeholders, visitors or service providers who may require access to computer resources.

c) File(s) – Any digital document or file, including (but not limited to) text, audio, video and image files, compressed archives or program files, scripts or libraries.

Scope

The terms of this policy are designed to protect the safety of all Users. This policy identifies those Users with particular responsibilities to maintain this protection.

Purpose

The Internet and digital communications are an essential element in the 21st century for education, business and social interaction. The school computer system and Internet access is designed expressly for student use and will include filtering appropriate to the age of the students. Clear boundaries will be set for the appropriate use of the computer system, the Internet and digital communications; these will be discussed staff and students. Staff will be made aware of, and pupils will be educated, in the safe use of the internet.

General Principles

Computer Resources are valuable assets that are provided to support both the education of students and the smooth running of the school. It is the responsibility of the School to ensure all Users, and particularly young people, use these Computer Resources in ways which will keep them safe, without limiting their opportunities for creativity and innovation. A number of precautions have to be taken to help ensure that the Systems are used responsibly and appropriately to maintain the wellbeing and safety of all Users.

Breaches of this policy will be dealt with in whatever manner is deemed appropriate and relevant by a member of staff who is considered appropriately placed to deal with the nature and severity of the breach.

Additional Relevant Policies and Procedures

- Acceptable Computer Use Policy
- Student Internet Policy
- Staff Internet Policy
- Student E-mail Policy
- Staff E-mail Policy
- Website Policy
- Software Policy
- Safeguarding policy
- Bullying Policy
- PSHE Policy
- Scheme of Financial Administration(SOFA)- Relating to SIMS
- Data Protection Act
- Social Networking Guidance

Requirements

To ensure e-safety can be maintained and monitored, all staff, students and parents or carers of students must read and sign that they have read and agree with the following:

- Acceptable Computer Use Policy
- Staff/Student Internet Policy
- Staff/Student E-mail Policy

Staff Roles

Role	Responsibility	2012/2013
E-Safety overview	Curriculum Deputy	A. Finch
E-Safety monitoring	ICT Network Manager	C. McKay
Safeguarding	Pastoral Deputy	A. Hudson
Student Guidance on ICT Use	E-Learning Manager & Head of ICT	C. Slater & J. Talbot
Student Guidance	SLT & Head of PSHE	A. Hudson, D. Fletcher, S. Rowland
Ensuring e-safety when using technologies and communications	All Staff	All staff

E-Safety Overview

Responsible for:

- Ensuring 'E-Safety Policy' is written and regularly reviewed
- Ensuring policy complies to all regulations regarding e-safety and safeguarding young people
- Ensuring procedures are regularly reviewed for effectiveness
- Monitoring the responsibilities of the manager for e-safety monitoring
- Conducting weekly checks on monitoring data
- Following all policies related to e-safety
- Reporting serious issues to the relevant authority
- Ensuring all staff receive appropriate training on e-safety
- Ensuring personal details and contact information are not available on the website or the VLE, and students' photographs are only used carefully and with permission from parents.

E-Safety Monitoring

Responsible for:

- Following the procedures for system checks, including installing virus protection and updating regularly
- Keeping accurate records of monitoring software outputs
- Providing a weekly report to person responsible for E-Safety Overview
- Ensuring any issues identified are reported to the person responsible for E-Safety Overview, the designated person on the pastoral team and the member of SLT responsible for Safeguarding.
- Following all policies related to e-safety
- Reporting serious issues to the relevant authority

Safeguarding

Responsible for:

- Following procedures specified in the policy
- Following all policies related to e-safety
- Reporting serious issues to the relevant authority
- Recording incidents and the follow-up actions

Student Guidance on ICT Use

Responsible for:

- Planning lessons on e-safety as part of the ICT programme of study and ensuring their effective delivery. These lessons should include (but are not limited to):
    a) Educating students in the effective use of the Internet for research, skills of knowledge location, retrieval and evaluation
    b) Making students aware of how they can report abuse or any offensive or inappropriate contact and who to report it to
    c) Teaching students never to reveal personal details, or those of others, in electronic communications, nor arrange to meet anyone
    d) Education in the safe use of social networking systems and other electronic communication methods
    e) Education in security on the Internet, social networking and e-mail
- Reporting serious issues to the relevant authority
- Following all policies related to e-safety

Student Guidance

SLT responsible for:

- Safeguarding young people
- Planning and delivering assemblies on e-safety
- Planning and delivering assemblies on bullying (including cyber-bullying)
- Planning and delivering assemblies on mobile phone use
- Reporting serious issues to the relevant authority
- Following all policies related to e-safety

Head of PSHE responsible for:

- Planning and delivery of lessons on e-safety
- Planning and delivery of lessons on safety
- Planning and delivery of lessons on bullying (including cyber-bullying)

- Reporting serious issues to the relevant authority
- Following all policies related to e-safety

Ensuring e-safety when using technologies and communications

Responsible for:

- Monitoring the use of technologies and communications in lessons
- Reporting serious issues to the relevant authority
- Ensuring the use of Internet derived materials by staff and students complies with copyright law
- Teaching students to be critically aware of the materials they read and how to validate information before accepting its accuracy
- Ensuring the safe and secure use of the Internet, VLE, e-mail, video-conferencing and other Computer Resources in lessons
- Following all policies related to e-safety

Virus Protection

The School will ensure the safety and security of personal data from theft, damage or modification by viruses by installing and maintaining effective virus protection software on all Systems.

The School currently uses Microsoft anti-virus software which is maintained and automatically updated by Microsoft System Centre. This anti-virus product filters all computer traffic on the School's network and it scans any File that is accessed on a student or staff machine, including those opened from or saved to an external medium such as an external hard drive or USB memory stick. It quarantines any suspect files found to prevent them spreading across the network and is logged and monitored by Microsoft System Centre, which is checked on a regular basis by the ICT Network Manager and technical staff for any warnings that may warrant intervention.

The system also checks for programs running on student or staff machines that may demonstrate suspicious behaviour. This prevents viruses or malware altering software on computers that could be used to re-direct students to websites showing inappropriate content or stealing usernames and passwords. Any running program deemed suspect by the virus filter is logged on the System Centre and is checked by the technical staff to verify if the software is legitimate or rogue.

For devices that are removed from the School site, such as laptops and netbooks, the anti-virus will continue to run and provide protection outside of school. All virus definitions are automatically updated when the device next connects to the school network and all staff and students are instructed to bring their device with them on a daily basis which helps to ensure the virus database remains up-to-date.

Web Content Filtering

All Internet traffic is passed through the School's Threat Management Gateway (TMG) filter and is scanned for access to websites deemed inappropriate by Microsoft or Byrchall High School. Microsoft updates the blocked website list on a daily basis and currently has over 100,000 restricted websites; this database of sites can be added to or relaxed by Byrchall technical staff as appropriate. The filter also scans files and attachments downloaded from the Internet or the email system for possible inappropriate content that could disrupt the network. All this information is stored in the filter for 30 days and is checked on a daily basis for inappropriate website access, attempts to bypass the filter or attempts to download files not allowed by the ICT policies in place at the School.

A further level of web filtering, provided by Impero software, is enabled on all student laptops and netbooks. This also uses a list of blocked websites to restrict access to inappropriate material. This filtering system continues to operate outside of school, ensuring that students continue to receive a level of protection when using their devices at home. The list of blocked websites is updated each time the computer is connected to the school network and all students are instructed to bring their device with them on a daily basis which helps to ensure the blocked list remains up-to-date.

Monitoring of Computer Usage

Impero software and Sophos UTM is installed on all computers provided by the School and its primary function is to monitor and report inappropriate computer use. The system can monitor and record:

- Which computers have been accessed and when.
- All programs that have been accessed, even after they have been closed.
- When inappropriate words have been typed in any program (using a comprehensive list of inappropriate words, including common alternatives and abbreviations often used to attempt to circumvent the system). Any match to this list triggers a screenshot of the desktop, capturing the date/time and program used to type the phrase.

The system can also be used to apply restructions, such as which programs are allowed, on a whole-school or individual basis.

The violation logs are monitored regularly by the ICT technical support staff and any issues are investigated as appropriate.

Work Folder Scanning

Byrchall technical staff manually scan file servers for Files that should not be on the network such as games, music files, scripts, batch files and inappropriate images and videos.

Remote Access

Access to Computer Resources is available remotely through the web application portal, webmail system and VLE. All remote access is logged and monitored using the systems described above.

In addition, staff can access SIMS remotely. Staff can only access SIMS remotely by using their school laptop. This maintains security of the data. All staff laptops have been encrypted and staff are required to lock their laptop away in a cupboard each evening if it is left in school. Staff may only carry sensitive data on mobile media devices which have been encrypted. Staff have been made aware of the Data Protection Act.

Parental Reporting and Data Access

All parents and carers are given access to student attendance, progress, behaviour and achievement data via the VLE. VLE access is limited to authenticated users and guest access is not permitted. To maintain the security of student data, all parent passwords are only released either in person or via written letter which will only be despatched to the registered address kept in the School's records. This is to ensure the information only reaches the intended individual and the information will not be given out via telephone or email as with these it is harder to verify identity. Parent passwords cannot be reset via the website – all resets must be requested from the School and they will again be sent in the post.

Additional Documentation

- SIMS Access Control Document
- TMG Block List and Categories
- Impero Key Words List

Policy Maintenance

This policy will be reviewed annually and updated in line with any changes in guidance or regulation that may have occurred.

The School reserves the right to change the terms of this policy without prior notice.