PINNER
HIGH SCHOOL

Policy Essential Information

Title: **E-Safety and ICT Acceptable Use Policy**

Date Approved: **24th April 2018**

Last Reviewed: **April 2018**

Next Review: **April 2020**

Status: **Statutory**

Delegation: **Headteacher**

Review Frequency: **2 Years**

Policy Locations: **SharePoint**

Version number:	1.2		Target Audience:	All staff / governors / parents and carers
Date authorised:	24th April 2018		Reason for version change:	Review Cycle
Date of next review:	April 2020		Name of owner/author:	Jennie Smyth – Deputy Headteacher

PINNER
HIGH SCHOOL

E-Safety and ICT Acceptable Use Policy

Statement of intent

This policy has been developed to ensure that all adults at Pinner High School are working together to safeguard and promote the welfare of young people.

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them. Annex C of Keeping Children Safe in Education refers specifically to online safety and should be read in conjunction with this policy.

This document aims to put into place effective management systems and arrangements, which will maximise the educational and social benefits that can be obtained through the use of ICT, whilst minimising any associated risks. It describes actions that should be put in place to address any concerns about student welfare and safety as well as how to protect young people and staff from risks and infringements.

The Headteacher or, in their absence, the authorised member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of students in their care.

The purpose of internet use in school is to help raise educational standards, promote student achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide young people with quality access as part of their learning experience and curriculum.

A risk assessment will be carried out before young people are allowed to use new technology in the school.

Ethos

- It is the duty of the school to ensure that every student in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world;
- Safeguarding and promoting the welfare of students is embedded in the culture of the school and its everyday practice and procedures;
- All staff have a responsibility to support e-Safe practices in school and all students need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols;
- E-safety is a concern that is not limited to school premises, school equipment or the school day;
- Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber-bullying will be dealt with in accordance with the school's policies on behaviour and preventing and responding to bullying;
- Complaints related to child protection will be dealt with in accordance with the school's child protection policy.

The Headteacher of Pinner High School will ensure that:

- All staff are included in e-safety training and that the training is integrated, aligned and considered as part of the school's overarching safeguarding approach. Staff must also understand that misuse of the internet may lead to disciplinary action (as detailed in section 5 of the HR Policies) and possible dismissal;
- A Designated Senior Member of Staff for e-learning /safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Child Protection;
- All temporary staff and volunteers are made aware of the school's e-learning /safety policy and arrangements;
- A commitment to e-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on e-learning/safety within the school;
- Procedures are in place for dealing with breaches of e-safety and security;
- All staff and volunteers have access to appropriate ICT training.

Teaching and learning

Benefits of internet use for education:

- The internet is a part of the statutory curriculum and a necessary tool for staff and students and it benefits education by allowing access to worldwide educational resources including art galleries and museums, as well as enabling access to specialists in many fields for students and staff;
- Access to the internet supports educational and cultural exchanges between students worldwide and enables students to participate in cultural, vocational, social and leisure use in libraries, clubs and at home;
- The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data;
- The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives;
- The internet offers opportunities for mentoring students and providing peer support for them and their teachers;
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation;
- Students will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Students will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance;

- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Managing the internet

- Developing good practice in internet use as a tool for teaching and learning is essential. School internet access will be designed expressly for student use and will include filtering appropriate to the age of the young people;
- Students will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide students on-line activities in class that will support the learning outcomes planned for the student's age and maturity;
- Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening;
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Technician and SLT;
- The school will ensure that the use of Internet derived materials by staff and students complies with copyright law;
- Students will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

Managing email

- Personal e-mail or messaging between staff and students should not take place;
- Staff must use the school e-mail address if they need to communicate with students about their school work e.g. study leave, course work and only fully trained e-mentors should contact students via email and only ever using the appropriate medium through SIMS Learning Gate/ Show My Homework;
- Students and staff may only use approved e-mail accounts on the school system and students must inform a member of staff immediately if they receive an offensive e-mail;
- Students must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone;
- Access in school to external personal e-mail accounts may be blocked;
- Excessive social email use can interfere with learning and will be restricted;
- The forwarding of chain letters is not permitted;
- Incoming email should be monitored and attachments should not be opened unless the author is known.

Managing website content
(and content on SIMS Learning Gate/ Show My Homework)

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a GDPR and security viewpoint including the use of photographic material;
- Photographs of students will not be used without the written consent of the student's parents/carers;

- The point of contact on the school website will be the school address, school email and telephone number. Staff or students' home information will not be published;
- The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate;
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing;
- Use of site photographs will be carefully selected so that any students cannot be identified or their image misused;
- The names of students will not be used on the website, particularly in association with any photographs;
- Work will only be used on the website with the permission of the student and their parents/carers;
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained;
- Students will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

Social networking and chat rooms

- The school will control access to moderated social networking sites and educate students in their safe use;
- Students will not access social networking sites such as 'Twitter', 'Facebook' or 'Bebo' on site;
- Students will be taught the importance of personal safety when using social networking sites and chat rooms;
- Students will not be allowed to access public or unregulated chat rooms;
- Students will only be allowed to use regulated educational chat environments and use will be supervised;
- Newsgroups will be blocked unless an educational need can be demonstrated;
- Students will be advised to use nicknames and avatars when using social networking sites off site;
- Staff will not exchange social networking addresses or use social networking sites to communicate with students;
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a student is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

Mobile phones and electronic devices

- We advise against bringing mobile phones to school. If students do bring them, mobile phones and other electronic devices must not be seen or heard during the school day or on the site at any time otherwise they will be confiscated and held in the school safe until the agreed return time.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's behaviour and preventing and responding to bullying policies;
- Students are not permitted to use the cameras in their mobile phones at any time;

- Staff will be issued with a school mobile phone where contact with parents or students is necessary, e.g. for school trips;
- iPads provided to staff must be used in accordance with the school's Acceptable Use Policy both within school and outside;
- iPads provided to staff are done so to be used for work/educational purposes only and thus all apps installed should be appropriate for use in school;
- iPads for students should go through the school's web filtering so as to monitor use and help prevent students accessing inappropriate material;
- Where photos are to be taken of activities involving students a school issued technology device should be used rather than personal technology;

Filtering

- The school will work in partnership with parents/carers, the DfE, partners and the Internet Service Provider to ensure that systems to protect students and staff are reviewed and improved regularly;
- If staff or students discover unsuitable sites, the URL and content must be reported to the ICT Technician and SLT;
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk);
- Regular checks by senior staff will ensure that the filtering methods selected are appropriate, effective and reasonable;
- Filtering methods will be age and curriculum appropriate.

Authorising internet access

- All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and the school's 'Acceptable Use of ICT Resources' document before using any school ICT resources.
- Any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site;
- The school will maintain a current record of all staff and students who are allowed access to the school's ICT systems.
- The school will maintain a record of students whose parents/carers have specifically requested that their child be denied internet or e-mail access;
- Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give permission for their child to access ICT resources;
- Staff will supervise access to the internet from the school site for all students.

Backups and Anti-Virus

- All content that is saved to a shared or personal drive located on a server is backed up to a local server regularly;
- The local backup server regularly replicates backups to a secure datacentre hosted by European Electronique;
- All computers in the school have an anti-virus program with real time scanning installed to prevent any damage or data loss caused by malicious files or programs;
- It is advised that staff do not use USB sticks to further limit the risk of infection.

Assessing risks

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. All staff should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored. Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

Rules for Internet access will be posted in all rooms where computers are used. Responsible Internet use, covering both school and home use, will be included in the curriculum. Students will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet. Students will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

Consulting staff

It is essential that teachers and other adults working at the school are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies. All staff are governed by the terms of this policy and will be provided with a copy and its importance explained. All new staff will be given access to a copy of the policy during their induction. Staff development in safe and responsible use of the internet will be provided as required. Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential. Senior managers will supervise members of staff who operate the monitoring procedures.

Maintaining ICT security

Personal data sent over the network will be encrypted or otherwise secured. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mails. The ICT technician will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

Parents/carers and students will work in partnership with the school staff to resolve any issues. As with issues to do with substance misuse, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff;
- Informing parents/carers;
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework;
- Exclusion;
- Referral to the police.

Monitoring, evaluation and review

This effectiveness of this policy is regularly monitored through the school's self-evaluation schedule.