WEST LANCASHIRE COMMUNITY HIGH SCHOOL

RESPECT ACHIEVE
SUCCESS FRIENDSHIP

WLCHS

Staff

Acceptable Use Policy

-Social Networking

-Social Media & Communication with students

-Cyber Security

2023-2024

Contents

PART 1- Staff Acceptable Use of the Internet and Digital Technologies

Policy Rationale

The internet is an essential element of modern life for education and social interaction. The purpose of internet use in school is to promote child achievement, to support the professional work of staff and to enhance the school's management, information and business administration system.

Benefits include: ·

- Access to worldwide resources and research materials ·
- Educational and cultural exchanges between Students worldwide
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The computing curriculum requires Students to learn how to locate, retrieve and exchange information using digital technologies whilst staying safe online. Consequently, in delivering the curriculum teachers need to plan to integrate the use of digital technologies and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill and also used as an essential home/school teaching and learning tool whilst including a common thread of online safety throughout its use as part of the curriculum.

Aims

Access to the school's network and use of digital facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy.

The Aims of this Acceptable Use Policy are to: -

- Allow all users access to school digital resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and Students are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990, General Data Protection Regulation (GDPR) 2018 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school and via Remote Access which are consistent with the general policies of the school.
- **Keep in line with KCSIE 2022 requirements for safeguarding children and maintaining a secure network.**

General Internet Use and Consent

Internet Use:

Students and parent(s)/carer(s) should agree to and sign the Home School Agreement each academic year. before being allowed to use the ICT facilities and accessing the internet. The signed forms will be kept on CPOMS for each student.

Students who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material. Students must not use the school digital facilities without the supervision of a member of staff.

Although use of the digital facilities and access to the Internet will be supervised and all possible measures will be taken, West Lancashire Community High School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or Students discover unsuitable sites, the URL (address) and content must be reported to the ICT Co-Ordinator immediately, who will, in turn, record the address and report on to the Internet Service Provider.

Students are aware that they must only access those services they have been given permission to use. Staff and Students are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)

Staff must agree to and sign the Acceptable Use Agreement (See appendix) each year.

Consent

Every year written permission from parent(s)/carer(s) will be sought on:

1. Use of their child's photograph in:

School Brochures

School Displays

School website

Press

Social Media

2. Use of their Child's video on:

School website

Social Media

The use of the names of Students will not be used on our School Website, School brochures, Press, Social Media.

On displays around school (Classrooms/Hall/Subject specific rooms) only the first name of pupils may be used.

Every Year written permission from employees will be sought on:

- School to use my photo in displays in school.
- School to use my photo on the school website.
- School to use my photo in the school newsletter/brochures
- School to use my photo in social media.
- School to share my photo for use in the media
- School to video me teaching

Filtering and Monitoring of Internet Sites

West Lancashire Community High School is in a contract with LCC EDS (Lancashire County Council Education Digital Services) for their internet and Broadband service and as such manage the internet filtering service. The product used by LCC EDS is Netsweeper and are using this on their Broadband connection, and schools have the ability to manage their own level of filtering and can run reports on usage.

The Netsweeper features include:

- Filtered Internet This is designed to categorise http and https traffic into over 90 easily identifiable categories so that school administrators can easily allow and block content. Real-time categorisation of websites occurs via Netsweeper Artificial Intelligence Engine and URL database, containing over 10 billion URLs, adding over 22 million new URLs each day.
- SSL (Secure Socket Layer) Inspection Decryption of SSL packets to ensure all internet requests are filtered, with the exception of a do not decrypt list containing financial and other trusted sites.
- User Identification; Multiple methods of user identification, through installed agents or I.P address. This enables schools to deliver a granular filtering experience, as well as being able to easily identify users of the internet for reporting and alerting purposes.
- Web Console Centralised, web-based administration console that enables support staff to manage Internet access policies, system administration rights, and reporting
- Proxy anonymizer detection. Some users have historically used anonymous proxy servers as a means of bypassing internet filters. The Netsweeper product can detect traffic that is trying to go via one of these servers and will block that traffic.
- Embedded web threat scanning capabilities, capable of identifying and blocking zero-minute and known web borne viruses, spyware, malware, and other forms of malicious code

The ICT Co-ordinator manages the catalogue of websites that are accessible to students, staff and visitors. Any requests for websites to be made accessible are authorised by the ICT Co-ordinator, who is a Senior Leader and the School DSL.

Cyber Security- Log in and Passwords

- Students and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Students and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- Staff and Students must ensure terminals, laptops or iPads are logged off (or hibernated) when left unattended.
- All staff iPads and laptops will have a uniform password that is shared only with members of staff.

- Ensure School cyber security training is completed, maintain strong passwords and maintain vigilance around security of school digital systems and personal data and online presence

Adult users are expected to manage their own areas on the network where relevant.

Passwords are therefore set for each user in these circumstances. We recommend that passwords are changed regularly

To protect your work area do not tell anyone your password. The password is displayed on screen as a line of ******, however people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful. Anyone who needs assistance in changing their password should contact the ICT Support technician or ICT Co-Ordinator. Teaching iPads will be used only for the purpose of teaching; no staff will access their emails via their teaching iPad for safeguarding purposes. SLT iPads will have different passwords to ensure emails cannot be accessed by other members of staff or Students.

General Safety and Risk Assessment

The consumption of food is forbidden whilst using a computer. It is hazardous to the equipment and to individuals. Users must treat equipment and services in school and at other sites accessed through school facilities with respect and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Risk assessments are completed for use of PCs and laptop trolleys and are kept in the ICT Suite. Staff are responsible for sharing the safety issues with their Students. Staff are responsible for the care of their iPad and laptop; including the transportation and use of equipment at members of staffs' homes.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets.

Adults need to help Students and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media Students can be cyber bullied 24 hours a day
- People who cyber bully may attempt to remain anonymous
- Anyone of any age can cyber bully
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient

Prevention

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe practice into all our teaching and learning, incidents can be avoided.

We recognise that we have a shared responsibility to prevent incidents of cyber bullying. The Head Teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Record Keeping and Monitoring Safe Practice

The ICT Co-ordinator/DSL keeps records of cyber bullying. Incidents of cyber bullying will be followed using School/ Local Authority procedures.

Online-Safety

Online-Safety is recognised as an essential aspect of Computing curriculum and the aim is to embed safe practices into the culture of the school.

The overall responsibility for Online-Safety has been designated to our DSL and ensure they keep up to date with Online-Safety issues and guidance through liaison with the Local Authority LADO and through organisations such as ThinkUKnow and The Child Exploitation and Online Protection (CEOP).

All Staff (all teachers, supply staff and teaching partners) are reminded/ updated about Online Safety matters at least once a year and usually more often, including in-depth understanding during safeguarding training. Students are regularly informed about e- safety through planned whole school and class assemblies and as an ongoing aspect of the computing curriculum. This includes an Online-Safety week in which Students explore and understand cyber-bullying and discuss how to tackle it if they encounter it. Any work or activity on the Internet or school equipment must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.

Users must not give out personal email or postal addresses, telephone numbers of any person. Under no circumstances give email or postal addresses / telephone numbers of any teachers or Students at school.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by Students and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

Users must not download, use or upload any material that is subject to copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material. Users should assume that ALL software is subject to copyright restrictions, including shareware.

Students must not, under any circumstances download or attempt to install any software on the school computers or IPADS. Staff should seek the advice of the ICT Support technician or the ICT Co-ordinator before attempting to download or upload software. Under no circumstances should users view, upload or download any material that is likely to be unsuitable for Students or schools. This applies to any material of violent, extremist, homophobic, dangerous, racist, or inappropriate sexual content.

If users are unsure about this or any materials, users must ask the ICT Co-ordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

All Students are aware of procedures to report any incidents of sexual or inappropriate content, radicalisation, extremism or anything else that worries them which they encounter during use of the internet. School staff will react appropriately and work with Students, parents and any other appropriate authority to resolve the issue.

Email Usage

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

When using e-mail, staff should:

- Not access personal emails in school using school equipment
- Be aware that e-mail is not a secure form of communication and therefore Students should not send ANY personal information
- Not attach large files
- Not forward e-mail messages onto others unless the sender's permission is first obtained
- Not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send e-mail messages in the heat of the moment and avoid writing anything that
- may be construed as defamatory, discriminatory, derogatory, rude or offensive
- Not open e-mail attachments from unknown senders or from computers from which
- virus protection may not be current or activated

This Guidance will apply to any inter-computer transaction, be it through web services, chat rooms, bulletin and news groups, blogging or peer to peer sharing.

Mobile Devices

Students are permitted to bring a mobile device to school, however during daytime, the mobile device is turned off and given to the School Office and are distributed at the end of the day.

Students may not make personal calls or send or receive email or text messages from or to a mobile phone during the school day. Mobile phones may not be used to take pictures of Students and staff (use iPads provided by the school). Students should not send or receive email or text messages to/from their mobile device during the school day.

Any child who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day. Any inappropriate use of mobile devices such as cyber bullying must be reported to the ICT Co-ordinator.

Staff should only use their mobile phones at appropriate times of the day only e.g. break times when there are no Students present. During the school day their mobiles should be turned off or set to silent and locked away for Safeguarding purposes. Staff must not use personal mobile devices or cameras to take images of Students or staff.

Acceptable emergency use:

- School trips where staff may need to contact a member of senior leadership may

- occasions where staff need to take photos on phone but must instantly delete / send across

and show another staff member that this has happened

- Emergency incident on site where a member of senior leadership is needed

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

School Network and Child Files

- Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Where provision allows, Students can access and save work to their own log-on through the server; this can only be accessed by that child, the class teacher, the Computing Leader and the ICT technician.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT Support technician will view any material Students store on the school's computers.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask their teacher or ICT technician for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician.
- Users accessing software or any services available through school facilities must comply with license agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network is accessed from home, this Acceptable Use Policy applies.

Use your Network Area or Cloud Storage

Where provisions apply, always ensure that files are saved to your network area NOT on the local hard drive. This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Home Documents

The school cannot accept responsibility for personal documents held on school laptops, it is the responsibility of the user to backup documents created at home or stored on the Home Docs of the laptop. It is recommended that staff do not keep personal documents on school devices.

Off site child data and child information

Laptops may be taken off site where agreed by the Head teacher. Staff are to ensure that no child data/information is downloaded from emails whilst off site and that pupil data is only accessed through the Remote Access facility-Secure Global Desktop. All devices must be logged off when left unattended.

Images taken on IPADS/Cameras must be transferred to the school network as soon as possible and be removed within the Academic year in which they were taken. Data, images and child information must be removed from backups and laptops when Students transfer to another class to avoid records being kept of Students that are not taught by their former teacher.

Virus Checks

All computers in school have anti virus software, although very new viruses will not be found. If you suspect a virus, please report it to the ICT Co-ordinator straight away.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please discuss this with the ICT Co- Ordinator. Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head Teacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author’s copyright. “Acquisition” includes loading a copy of a programme into the random-access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

“Hacking” is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Students Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

If staff break the rules as laid down by this policy, they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken, the police will be informed, and the school will assist the police with any prosecution

Disciplinary Procedure for All School Based Staff

Employees are informed that disciplinary action may be taken in relation to those members of staff who conduct themselves in a way which is contrary to the advice and guidance outlined in this Policy. If such conduct is deemed to amount to gross misconduct this may lead to dismissal.

Additional Information

Please be aware, at such time that you leave West Lancashire Community High School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

If you do not understand any part of this Acceptable Use Policy, please ask the Head Teacher for further guidance

PART 2 –

Social Networking and Social Media and Communication with Pupils Policy Rationale

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both Students and themselves.

Application

This Policy applies to all staff employed in delegated schools and those Teachers employed in Centrally Managed Services.

Background

The use of social networking sites such as Facebook, Twitter, Pintrest, LinkedIn and MySpace has over recent years become the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, Instagram and Snapchat.

Guidance and Advice

Employees who choose to make use of social networking site/media should be advised as follows:-

(i) That they should not access these sites for personal use during working hours;

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

(iii) That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- lead to valid parental complaints;
- be deemed as derogatory towards the school and/or it's employees;
- be deemed as derogatory towards pupils and/or parents and carers;
- bring into question their appropriateness to work with Students

(iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(vi) That they could face legal proceedings if comments they post about named individuals are found to have harmed their reputation.

*(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure.)*

KCSIE 2022: Schools will access social networking sites in order to 'vet' prospective employees.

Part 3- Remote Learning

Communication with Pupils

Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc.

Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
staff and pupils should be in living / communal areas – no bedrooms
staff and pupils should be fully dressed
filters at a child's home may be set at a threshold which is different to the school resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required. If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

Remote access

We allow senior staff to access the school's ICT facilities and materials remotely.

We use Teamviewer which uses an industry-recognised AES 256-bit encryption standard as well as 'brute force protection'. Staff users are protected when accessing or sharing potentially sensitive information by a two part logging in protocol which randomly generates user name and numbers each time it is accessed. Access is allowed through the Senior Leadership Team and any issues reported to the IT Manager.

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 and take such precautions

Our 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 the WLCHS data protection policy.

School social media accounts

West Lancs Community High school has an official Facebook page. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of school network and 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, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/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, legal obligation or Freedom of Information Act request.

PART 4 Staff Agreement Form

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.

- I understand that I need to obtain permission for children and young people before they can upload images (video or photographs) to the internet or send them via E- mail.

- I know that images should not be inappropriate or reveal any personal information of children and young people.

- I have read the procedures for incidents of misuse in the Internet and Digital Technology Acceptable Use

- Policy so that I can deal with any problems that may arise, effectively.

- I will report accidental misuse.

- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person in accordance with procedures listed in the Acceptable Use Policy.

- I know who my Senior Designated Person is.

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones to contact parents.

- I know that I must not use the school system for personal use unless this has been agreed by the Head Teacher.

- I know that I should complete virus checks on my ipad /laptop and other storage devices; including regularly installing updates on to school devices, so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

- I will ensure that I follow the Data Protection Act 1998 and GDPR 2018 and have checked I know what this involves.

- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Head Teacher prior to sharing this information.

- I will adhere to copyright and intellectual property rights.

- I will only install hardware and software I have been given permission for.

- I will ensure the safe keeping of school equipment if I take it off the school premise. I will be responsible for loss and damage.

- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden.

- I understand that intentional violation of this rule may result in disciplinary procedures being initiated.

- I have read, understood and agree with these Agreements as I know that by following them I have a better understanding of e-safety and my responsibilities to safeguard children and young people when using online technologies.

- **I have completed the National Cyber Security Centre training 2023**

- **I have read and signed Part 1 of Keeping Children Safe in Education 2022**

Signed ____

Date____

Name in Print____