Online safety policy

PENDLE VALE COLLEGE

Approved by:	Steve Wilson	**Date: December 19**
Last reviewed on:	December 2019	
Next review due by:	December 2020	

Contents

……

1. Aims

Our college aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any flagged/seached queries that are deemed a safeguarding concern are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are referred to the appropriate person in college to deal with in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers (where applicable) are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community are only allowed access to the college IT infrastructure with direct permission of the ICT Manager.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming website and during other forms of online activity.

Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents *in confidence/anonymously* and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident and material is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material or activity, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

This will be recorded on CPOMS.

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors to ensure they comply with the above and our legal duties. More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Students may bring mobile devices into school, however they must be switched off at the school gate and are not to be accessed at any point during the school day without the permission of a member of staff.

Any use of mobile devices in school must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement, by a pupil, will trigger disciplinary action in line with the school behaviour policy. This may result in the confiscation of their device.

9. Staff using work devices off Campus

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing school data must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

10. How the school will respond to incidents of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device whilst on campus where such action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through regular emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding & Child Protection Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed annually by the Headteacher. At every review, the policy will be shared with the governing body

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding & Child Protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable use agreement (students and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will:

- Treat all equipment with respect and keep it clean and tidy, taking special care when using laptops and iPads as these are easily damaged.
- Always use the PC, iMac, laptop or iPad you have been allocated by my teacher. I will be responsible for this during the lesson and will be accountable for any damage to it.
- Tell a teacher straight away if you notice anything wrong with the equipment.
- Always log in properly using my own user name. I must never log into someone else's account or access their files.
- Take care to keep my passwords secure and never give them to anyone else. Change all default passwords at the first opportunity and choose new passwords you can easily remember.
- Always lock my account before leaving a machine unattended.
- Never attempt to access or use staff devices/accounts.
- Save files in my own area with sensible and appropriate filenames. Files with unsuitable names (e.g. containing bad language) or with inappropriate content will be deleted with no forewarning.
- Promptly delete files I no longer need and organise files I am keeping in folders with suitable names.
- Tell a teacher straight away if someone has been tampering with my files or knows any of my passwords.
- Not use the College system for personal use without specific permission from the Headteacher. This includes accessing or attempting to access personal email/social networking accounts and storing personal files – e.g. images, music, videos, etc.
- Always have permission from a member of staff to use the network or internet and must always use it responsibly.
- Always respect copyright and intellectual property rights when using information from the internet.
- Always use my email account responsibly and only use it for schoolwork.
- Always have permission from a member of staff to use blogs, discussion groups and similar forums.
- All messages must be written carefully and politely. Remember that they may be seen by unintended readers.
- Anonymous messages and chain letters are not permitted.
- Take care to not give out personal information through email, blogs or any other electronic means.

These responsibilities apply when using Moodle, email and other College based ICT facilities outside College.

ICT use may involve photographic, video or audio recordings being created, please make a teacher aware if you object to being included in such media or are aware of external circumstances that restrict you being included. Students should not record or photograph anyone without their permission and/or knowledge.

Portable ICT equipment in my care should not be left unattended anywhere in school, if you discover unattended portable ICT equipment (pen drive, iPad, laptop, etc.) it should be passed immediately to a member of staff.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use at anyone point whilst on the school campus or during other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

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 responsibly.

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 students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I:

- Will respect system and network security and I will not disclose any password or security information to anyone other than in exceptional circumstances when I will seek prior permission from the ICT Manager or Head Teacher.
- Will not share any personal data, concerning an individual or group, with any third party without the prior approval of the Data Protection Officer (DPO).
- If I become aware that a third party no longer requires access to any particular personal data, is using it for reasons other than those previously agreed and/or is in possession or receipt of personal data that they should not have I will notify the Data Protection Officer as soon as possible.
- If I become aware that any personal data is inaccurate (e.g. wrong phone number, address, etc.) I will notify the Data Protection Officer as soon as possible.
- Will not retain personal data for longer than is necessary to perform my duties.
- Will not attempt to access the personal files and/or communications of others unless given permission by the owner or directly requested to do so by the ICT Manager or Head Teacher.
- Will not install any software or hardware without permission. (*See Pendle Vale College Staff ICT Device Agreement for further information specifically relating to staff devices.*)
- Will ensure that personal data is stored securely and is used appropriately, whether in college, taken off the college premises or accessed remotely. I will never store private, confidential and/or sensitive data on unencrypted/unsecured media (e.g. USB pen drives, external hard drives, CD/DVD, etc.) or any device that has not been approved by the Data Protection Officer, ICT Manager, or Head Teacher (e.g. personal computers).
- Will respect copyright and intellectual property rights and seek guidance if I am unsure.
- Will report any incidents of concern regarding children's safety to the Designated Senior Person.
- Will ensure that electronic communications with students are conducted in accordance with my professional role and will do my best to ensure that messages cannot be misunderstood or misinterpreted.
- Will promote e-safety with students in my care and will help them to develop a responsible attitude to ICT use, communications and publishing.
- Will use my college email address for all communication, both internal and external, relating to my professional role and will ensure that secure copies are kept of emails containing information which may later be needed by myself or someone else, including outside agencies.
- Will not use my college email address for personal communication.
- Will ensure that I log off or lock any computer before leaving it unattended.

- understand that transmitting or electronically publishing material, including via social networking sites, which may damage the reputation of the college or bring it into disrepute could result in disciplinary action.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and may also include personal ICT devices when used for College business or when connected to College systems.

If I am in doubt or have any questions regarding the use of ICT or the handling of personal data I will always seek the guidance of the ICT Manager and/or Data Protection Officer prior to undertaking any task or use.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them 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 ensure that students in my care do so too.

The College may exercise its right to monitor the use of the College's ICT systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the College's ICT system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Acceptable Use Policy for ICT

Signed (staff member/governor/volunteer/visitor):	**Date:**

ICT devices (including, but not limited to, laptops and iPads) are made available to staff for their own professional use. It is expected that this may include use at various locations including the member of staff's home. The following points apply to all devices issued to staff:

1. Devices remain the property of Pendle Vale College.
2. School policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the device. Staff are responsible for ensuring any person using a device, either in college or off site, only uses it for appropriate activities and in accordance with this agreement.

3. Staff must never allow students to use their devices.
4. College issued devices should never be left on a floor, the edge of a worktop or other location where there is a high likelihood of accidental damage occurring.
5. Any faults with a device are to be reported to the ICT Manager or the Business Manager. Under no circumstances should staff attempt to fix suspected faults themselves.
6. Pendle Vale College Software:
   a. Software installed on devices at the time of issue is licensed to Pendle Vale College and is recorded in the College Licensing Database.
   b. Staff must not install any further software, owned by Pendle Vale College, without express permission. Requests for any further College software must be made to the ICT Manager.
7. Staff may install their home broadband and printer on their device(s) but must not install any other software without first consulting the ICT Manager. Please note:
   a. Staff will be personally liable for any issues relating to illegally downloaded/installed content, including music and/or video that is subject to copyright.
   b. If a device has to be restored to its original state, all personal software will be lost as will all personal files which are not backed up.
8. Use of devices away from college premises:
   a. Devices are covered by the college insurance and staff should not include them in their home insurance.
   b. Staff must take all reasonable precautions to prevent devices being stolen or otherwise damaged.
   c. Devices should not be left in an unattended vehicle unless it is absolutely necessary, if it is unavoidable, they should be locked away out of sight and the vehicle fully secured.
   d. Devices should be carried in secure and robust carrying cases so as to minimise the risk of accidental damage and should never be left unattended by the staff member.
   e. Staff must ensure that student and other sensitive data is secure at all times and not accessible to any third party. Staff must not copy such data from their device to USB pen drives and/or external hard drives.
   f. Staff are responsible for any charges incurred while using devices to access the internet off campus.
   g. Staff should ensure that personal files are not stored on the network or in other work-related storage areas (e.g. Dropbox account, etc.).

Data Protection / Security

1. All passwords must be retained securely and must not be disclosed to anyone. Passwords must not be written down in a manner which may disclose them to another person.
2. Initially passwords may be set to a default password, as may those which have been reset by an administrator. You must change these passwords immediately as default passwords may be known by others, including students.
3. You must take every precaution to protect data when logged onto a device in a classroom and at any time when students are present. Student data / registers should not be projected and students should not be allowed access to staff devices.
4. Users should not leave a live session unattended: either log off or lock the device. This will remove any opportunity for unauthorised use by another person, including students.

5. Every precaution must be taken to safeguard confidential and sensitive data. Such data must never be stored on unsecured and/or unencrypted USB pen drives, external hard drives or computers/systems not under the control of Pendle Vale College.
6. Staff must never allow students to use their logins or access a machine logged in with a staff account that will not be directly supervised for any period of time.
7. Staff are responsible for saving/backing up their files in a timely manner via any of the various means provided (e.g. Dropbox, Office 365, iCloud, Moodle, network drives, etc.). Any data not saved to/backed up via one of the available options, which has resiliency, may be irretrievable in the event of deletion, loss or hardware failure. Staff unsure of an appropriate method to back up their files should seek prompt guidance from the ICT Support team.
8. The College ICT Manager is ultimately responsible for the campus network. The use of personal devices in school is by agreement with the IT team. Failure to do so will be treated as a disciplinary matter.
9. If a member of staff wishes to use a device that will need to be plugged into College power sockets there is a requirement for it to be PAT tested. This is organised through Reception and Engie FM.

Long Term Staff Absence

If a member of staff is absent for a prolonged period of time, their device(s) will need to be returned for use by staff covering their absence.

1. In these circumstances the following process is followed: -

    a. Staff should remove any personal files and take their own backup of work related files prior to returning the device(s).
    b. All files saved on laptops in standard locations (e.g. Documents folder, Desktop, etc.) will be backed up to the network once the laptop is returned. Every effort will be made to ensure no files are lost but staff should be aware that files not saved in standard locations are at risk and cannot be guaranteed to be backed up.
    c. The device will usually be re-imaged. This means that any personal software such as home broadband, printer drivers and the like will be lost.
    d. When the member of staff returns to work, the device(s) will be reimaged to the default settings and any relevant files restored from backup, prior to the device(s) being returned to them.

I have read the guidelines for use of devices and agree to comply with them. I understand that devices may have monitoring software installed and that use of devices, both on and off campus, may be monitored.

I have read, understood and accept the Staff ICT Device Agreement
Signed
Date
Print name
Device Serial No.
Device Type