Pendle Community High School & College
Online Safety Policy (September 2017)

In general, online safety is regarded as SAFEGUARDING issues where technology is involved. To reduce these risks, online safety seeks to continually educate staff and students on how to improve their personal safety and minimise security risks to their private information and property when using technology online.

This online safety policy has been developed by a working group made up of: senior leaders, Online Safety Lead, staff – including teachers, support staff, technical staff, chair of governors and advice was also sought from the Lancashire Safeguarding Children's Board (LSBC). The school actively uses the South West Grid for Learning (SWGfL) '360° Safe Self Review Tool' for online safety to regularly review, inform and progress the school's online safety approach as part of its ongoing commitment to developing online safety provision for all members of the school community.

Consultation with the whole school community has taken place and this policy links into the wider Safeguarding and Child Protection policy of the school.

Scope of the Policy

This policy applies to all members of the school community (including staff, students , volunteers, parents / carers, visitors) who have access to and are users of school ICT systems. The system has an added level of security as the network guest password is not available freely and the ICT campus technician/s input any passwords directly should a guest log-in be required.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online incidents covered by this policy, which may take place outside of the school, yet is linked to the school. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data such as contact lists. In the case of both acts, action could be taken over issues covered within the published Behaviour Policy.

The school will deal with any such incidents within this policy and associated behaviour policies and will inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*:

Governors are responsible for the approval of the Online Safety Policy.

The Online Safety Lead along with the DSL lead the online safety group and

assume day to day responsibility for online safety issues. They have a leading role in establishing and reviewing the school online safety policies and documents, liaising with school technical staff and in providing training for staff

The Campus technical staff ensure that the campus technical infrastructure is secure and is not open to misuse or malicious attack and that the school meets required online safety technical requirements and any Local Authority Guidance that may apply. They ensure that users may only access the networks and devices through a properly enforced password.

Teaching and support staff are responsible for ensuring that they have an up to date awareness of online safety matters and of the current online safety policy and practices. Staff must have read, understood and signed the Staff Acceptable Use Policy (AUP) and report any suspected misuse or problems to the Online Safety Lead or DSL. Staff need to understand the requirements of Keeping Children Safe in Education (KCSIE) 2016 Part 1 and there must be no digital communications with students and any communication with/ parents / carers should be on a professional level using school systems only.

All staff should ensure that online safety issues are embedded in all aspects of the curriculum and that students are aware of and follow the online safety and acceptable use policies. Staff should monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.

In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. (The unsuitable sites are noted down in a hardback book.)

Students are responsible for using the school / digital technology systems in accordance with the Student / Pupil Acceptable Use Policy and need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Students are expected to be aware of the importance of rules around the use of mobile devices, digital cameras, taking / using images and of the implications of online bullying.

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and follow the procedures of the school when visiting.

<u>Education – students</u>

Online safety is reinforced in all areas of the curriculum.

A planned online safety curriculum is provided as part of Computing / PHSE and SRE.
Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
Students should be taught in all lessons to be critically aware of the materials / content they access online appropriate to their level of understanding.
Students should be made aware of the source of information used and to respect copyright when using material accessed on the internet
Students should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

Staff will act as good role models in their use of digital technologies, the internet and mobile devices
Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request via the Website Filter Bypass request that the Campus ICT technician can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and having sought permission from the subject lead and SLT. The campus uses BTLS Lightspeed filtering system which is monitored by the campus technicians and SLT informed of any unusual searches or issues.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
A planned programme of formal online safety training will be made available to staff. This will be regularly updated at least annually and reinforced termly.
All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days and additional training will be organised for the Online Safety Lead and DSL.

Training – Governors

Governors take part in online safety training and awareness sessions, with particular importance for those who are members of any sub- committee / group involved in technology / online safety / health and safety / child protection. Governors understand their responsibilities as outlined in KCSIE 2016.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure the school meets recommended technical requirements and Local Authority Guidance.
- There are ongoing reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and where possible, physical access restricted
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a personal username and secure password
- The bursar / school business manager along with campus technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Inappropriate content (e.g. websites hosting materials of a sexual/ drug/ violent nature etc.) is automatically blocked by the broadband and filtering provision. Content lists are constantly updated and internet use

is logged and regularly monitored (e.g. weekly reports of suspicious search queries, remote monitoring.) There is a clear process in place to deal with requests for filtering changes (see appendix website filter bypass.)

- The school provides enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc.)
- Campus technical staff regularly monitor and record the activity of users on the school technical systems and flag up any unusual searches to SLT.
- Any potential technical incidents or security breaches are to be immediately reported to SLT and the campus technician.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious activities which might threaten the security of the school systems and data. These are tested and reviewed regularly. The school infrastructure and individual workstations are protected by up to date anti-virus software.
- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may at times be used out of school and there are controls in place to restrict all users from downloading executable files and installing programmes on school devices. *(*see Appendix Staff AUP/ Staff Device Agreement)
- An agreed policy is in place (Staff AUP) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices especially in regard to the storage of sensitive data.

<u>Use of digital and video images</u>

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet and via social media. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The sharing of inappropriate or explicit images online via mobile phones, webcams, social media and instant messaging is known as sexting. (Young people often view this as a mundane or normal activity and part of flirting, but by sending an explicit image a young person is producing and distributing child abuse images and risks being prosecuted even if the image is taken and shared with permission.) Young people can also then be at an increased risk of blackmail, exploitation, bullying, emotional distress and unwanted attention. All members of staff must be aware that if any young person discloses that they have sent or received a ‘sext’ or ‘nude selfie’ that these images should not be printed, copied or forwarded. Staff should immediately inform the school’s DSL. The school has adopted the LSCB 'Sexting Process Guidance' for managing potential instances appropriately which is included as an Appendix to this policy. In addition, the DSL is expressly familiar with the UK Council for Child Internet Safety (UKCCIS) 'Sexting in Schools & Colleges' guidance for handling incidents of Sexting in a considered and appropriate manner in accordance with national guidelines.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Those images should only be taken on school equipment, the personal equipment of staff must not be used for such purposes.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)

Data Protection and Freedom of Information

The school has a Data Protection Policy ensuring that personal information is dealt with correctly and securely and in accordance with the Data protection Act 1998 and other related legislation. Please read this policy in conjunction with the

- School Data Protection Policy
- Freedom of Information Guidance)
- Information Commissioner's Office (ICO) Guidance
- Statement of Ethical Standards
- Code of Conduct for Delegated Budgets

Staff must also ensure that they:

- At all times take care to ensure the safe keeping of personal data, and follow the above policies and guidance, which will minimise the risk of loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data. Screen lock if leaving their computer unattended.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

Students follow the following rules during school hours.

Mobile phones may be brought to school for independent travellers and in other agreed circumstances for pupils where there is an identified need such as listening to music on transport. This is agreed with parents/ carers and SLT.

NO use of mobile phones in lessons or social time (except Post 16 social time)

NO taking photos on mobile phones / cameras

NO use of other mobile devices eg tablets, gaming devices

NO use of personal email addresses in school, or on school network

NO use of school email for personal emails

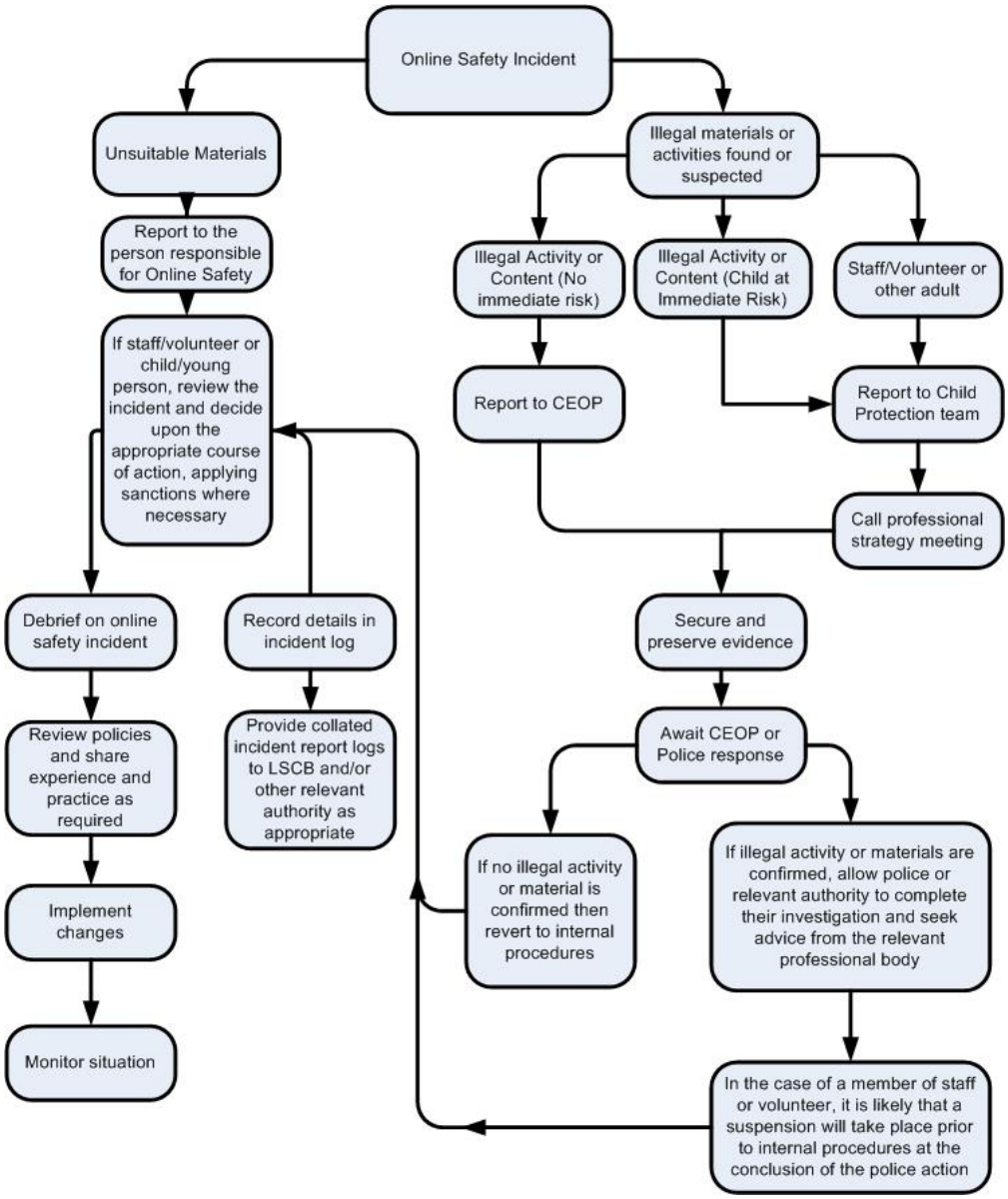
NO use of messaging apps, social media, blogs

When using communication technologies the school considers the following as good practice:

- The official school / email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school / policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school / systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Students and parents have been made aware of the website Whisper Button for anonymous reporting of any online bullying issues. Students are reminded of this regularly through assemblies, form time and online safety week.
- Personal information should not be posted on the school / website and only official email addresses should be used to identify members of staff.

<u>Illegal incidents</u>

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online safety incident procedure

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Two senior members of staff to be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store

screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated they will need to assess whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by Local Authority or national / local organisation
  - police involvement and/or action
  - if content being reviewed includes images of child abuse then the monitoring is halted and referred to the police immediately.
    Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- The computer in question should then be secured as any change to its state may hinder a later police investigation. Lancashire police guidance on suspected illegal activity is to remove the power at source. (I.e. pull the plug not shut down the equipment).

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection / safeguarding purposes. Any related documentation should be retained for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. (See Behaviour Policy / Staff AUP / Staff Device Agreement)

This policy should be read in conjunction with the school's: -
Child Protection and Safeguarding Policy
Positive Behaviour and SEMH Policy
Guidance for Safer Working Practice October 2015
Keeping Children Safe in Education September 2016
and the appendices indicated below.
School Data Protection Policy
Freedom of Information

Appendices:
Website filter bypass request
Staff Acceptable User Policy
Pupil Acceptable User Policy
Volunteer Acceptable User Policy
IPad AUP
Staff Device Agreement
Use of social networking sites Guidance LCC
Communication and social networking AUP

'Sexting in Schools & Colleges' guidance (UKCCIS)

Additional guidance and advice taken from:
UK Safer Internet Centre (UKSIC) including appropriate filtering and monitoring guidance
UK Council for Child Internet Safety (UKCCIS)
Lancashire Children's Safeguarding Board (LCSB)

Policy approved by Governors: 21st June 2017

Review date: June 2018

Signed: _____
(Chair of Governors)

Signed: _____
(Headteacher)