PENK VALLEY FEDERATION

On Line Safety Policy

To be Approved at Full Governing Body Meeting

April 2017

Frequency of Review: Bi annually

Policy based on : South West Grid for Learning template(SWGfL)

Amendments
2017 – Liam Meredith, Richard Davenport, Steve McCosh, NF/DS/HJ/JA/PJT – Federation SLT 8/03/2017

Scope of the Policy

This policy applies to all members of the Penk Valley Federation (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

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 cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. In order to support this, the termly Headteacher reports presented to the Full Governing body will include the following:

- Termly monitoring of Online Safety incident logs
- Termly monitoring of filtering / change control logs

Principal, Headteacher and Senior Leaders:

- The Principal/Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

	MFS	PFS	PMS	WHS
Online Safety Coordinator	**Mrs D Spiers**	**Ms R Cashmore**	**Mr L Meredith**	**Mr S McCosh**
Monitoring of on line reporting system	**Mrs D Spiers**	**Ms H Johnson**	**Designated Safeguarding Lead**	**Designated Safeguarding Lead/Deputy**
System Used in school	**PCE**	**PCE**	**E SAFE**	**E SAFE**

Designated Safeguarding Lead	**Mrs D Spiers**	**Ms H Johnson**	**Mr R West**	**Mr S McCosh**
Deputy Safeguarding Lead	**n/a**	**Mrs J Binns**	**Mrs S Hodson**	**Mrs S Wynn Ms C Edwards**
Network Manager	**Mrs J Ablewhite**	**Mrs J Ablewhite**	**Mrs J Ablewhite**	**Mrs J Ablewhite**

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (See flow chart on dealing with Online Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

Online Safety Coordinator will be responsible for:

- taking day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place. i.e. using Safeguarding Whistleblowing form
- providing training and advice for staff
- liaising with the Local Authority
- liaising with PVFl ICT technical staff
- Collating reports and investigating Online Safety incidents and creates a log of incidents to inform future Network Manager of future Online Safety developments
- reporting regularly to Senior Leadership Team
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression

Network Manager and Technical staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- meeting regularly with Designated Safeguarding Lead to discuss current issues and to review incident reports from PCE and ESafe, and on line filtering control logs.

Web Filtering

RM provides all Federation Schools with the filtering solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. Each schools is able to control their own permissions and add/amend to the defaults.

E-Safety System

Wolgarston High School and Penkridge Middle School use an online monitoring system called E-Safe which monitors, manages and protects anyone using ICT at school. Software on the computers sends data securely to the e-Safe monitoring personnel (who are all DBS cleared and

CEOP trained), they then send a daily report to the Designated Safeguarding Lead who can then deal appropriately with the user.

Marshbrook First School and Princefield First School use an online monitoring system called Policy Central Enterprise. This system filters through all the content that appears on the users computer, based on a series of built-in word/phrase libraries. If a user views or types inappropriate text, a full screen capture is taken in real-time showing all the things that they were doing at that time. This information can then be viewed by the Designated Safeguarding Lead who can then deal appropriately with the user.

The Penk Valley helpdesk can be contacted if schools require assistance with this using email - helpdesk@penkvalley.co.uk .

ICT Technicians are responsible for ensuring:

- the school's filtering policy as related to the above system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network, Virtual Learning Environment (VLE) where available, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Co-ordinator for investigation, action and if appropriate sanctions.
- that monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy agreement (AUP) (See Appendix C)
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation, action and if appropriate sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) if applicable should be on a professional level ***and only carried out using official school systems***
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- pupils understand and follow the school Online Safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of Online Safety issues related to the use of mobile phones and cameras and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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

Designated Safeguarding Lead

All DSL's are trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal or inappropriate materials;
- inappropriate on-line contact with adults and strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Note: it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Pupils:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.
- Pupils at Wolgarston High School and Penkridge Middle School (Appendix B) must sign the AUP before they are given access to the computer system. Students also have to accept the AUP on each login attempt before being able to access the school network, if they choose to decline it they will be automatically logged off.
- Pupils at Marshbrook First School and Princefield First School can choose to accept or decline the schools AUP when they log into a computer. If they choose to decline it they will be automatically logged off.
- will be expected to know and understand school policies on the use of mobile phones, and digital cameras. They should also know and understand school procedures on the taking use of images, cyber-bullying and use of mobile phones.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE (if available) and information about national / local Online Safety campaigns / literature.*

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy;
    - **Appendix A for Wolgarston High School**
    - **Appendix B for Penkridge Middle School (Normally found in Pupils Planner)**
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/ICT, will be age appropriate and should be regularly revisited
  - key online safety messages should be 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 on-line and be guided to validate the accuracy of information.
  - students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
  - students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
  - 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 should act as good role models in their use of digital technologies the internet and mobile devices
  - in lessons where internet use is pre-planned, it is best practice that 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.
  - 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff to 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.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers Online Safety evenings
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Review of Policy

This policy will be reviewed bi- annually by the Federation Governing Body.

Appendix A

June 2016

Dear Parent / Carer

ICT and Internet Use

As part of the school curriculum at Wolgarston High School, we offer pupils limited access to the Internet. Before being allowed to use the Internet, all students must obtain parental permission and there is a completion page enclosed, in the Data Collection Form booklet, for you to return.

The Internet is a global network of computers containing thousands of libraries, databases and bulletin boards that can support students' learning in all areas of the curriculum. However, parents should be advised that some material accessible on the Internet might contain items which are illegal, defamatory, inaccurate or potentially offensive to users.

During school time, teachers will supervise and guide students towards appropriate materials. The school's Internet Service Provider will employ measures to protect against access to inappropriate materials. Inappropriate use of computer systems is detected and monitored. Students using the resources inappropriately will be dealt with according to the sanctions of the school's Behaviour for Learning policy. These procedures should ensure that pupils only use the Internet to further educational goals and objectives.

We believe that any disadvantage of the Internet is outweighed by positive benefits to the pupils in enhanced learning opportunities. However, the school respects the right of each family to decide whether or not to apply for access.

Please find attached a copy of our ICT and Internet Use "Good Practice" rules which your son / daughter will be expected to follow, if you agree to use of the Internet. Each student will then be given an individual password and user area which, as stated in the rules, must remain secret so that it allows secure use only by the student.

Yours sincerely

Headteacher

Appendix A (WHS)

Responsible ICT and Internet Use

e-Safety in School

Wolgarston Commitment:

Wolgarston is committed to following the (ICT) Security Policy for Schools developed by Staffordshire County Council. This document is reviewed annually. The full details of this policy can be found by accessing Wolgarston High School web site: www.wolgarston.staffs.sch.uk and clicking on the 'About Us' tab and accessing School Policies. A hard copy of this is available upon request from office@wolgarston.staffs.sch.uk.

Wolgarston aims to provide a safe environment to all users and to support this we employ ESafe network monitoring. This provides us with detailed information of inappropriate activity of any network user. Inappropriate use is always acted upon, by reporting to the e-Safety Officer/Headteacher and any relevant external authorities.

For school purposes, Internet use encompasses email and any other messaging systems.

The e-Safety Strategy

Will:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give adequate information on where to seek help and how to report incidents.
- Ensure young people understand that there are sanctions that the school will impose on them if they act inappropriately when online.
- Provide guidelines for parents, carers and others on safe practice.
- Ensure policies are regularly monitored and reviewed with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.
- Students accept each time they access our system to abide by the policy

Student Guidelines for Internet Use

General

The Internet, primarily, is provided for students to conduct research and back up their work. Parent's / carers permission is required before a student is granted access. Access is a privilege not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communication over the network. Users must comply with school standards and honour the agreement they have signed.

Computer storage areas, including any external storage media brought to school, may be reviewed by staff to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.

Appendix A (WHS)

For school purposes, Internet use encompasses email and any other messaging systems.

During school, teachers will guide students towards appropriate materials. Outside of school, families bear responsibility for such guidance in the same way as they deal with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted within the school environment:

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Accessing inappropriate web sites
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws.
- Using others' passwords or accounts.
- 'Hacking' into others' folders, work or files for any reason.
- Intentionally wasting limited resources, including printer ink and paper.

Sanctions

1. Violations of the above rules **will** result in a temporary or permanent ban on internet/computer use. The school runs a system which reports inappropriate use and operates at a high level of accuracy.
2. Your parents/carers will be informed.
3. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
4. When applicable, police and/or local authorities will be involved.
5. If necessary, external agencies such as Social Networking or Email Member sites will be contacted and informed.
6. A record of all unacceptable use will be kept and reported to Senior Management.

Individual Students

1. You must have your parent's/carer's permission before using the Internet.
2. You must have a supervising teacher or member of staff with you at all times when using the Internet.
3. Do not disclose any password or log-in name to anyone, other than the persons responsible for running and maintaining the system.
4. Do not upload/send personal addresses, telephones/fax numbers or photographs of anyone (staff, governors or students) at the school.
5. Use of names of students, or photographs of students, will require parents to have been informed about such use.
6. Do not download, use or upload any material which is copyright.
7. Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children and young adults. This applies to any material of a violent, dangerous or inappropriate context. If you are unsure always ask a member of staff.

8. Always respect the privacy of the files of other users.
9. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything that could be interpreted as libel.
10. The internet will be used for appropriate educational use only. Access to Internet games or social network sites is prohibited.
11. Ensure that you have followed the correct procedures for using the Internet and report any incident which breaches these rules to a member of staff. Any messages received which are offensive should be reported to a member of staff.
12. **Never take any action liable to bring Wolgarston High School into disrepute.**

Please note that this policy is produced in line with accepted DfE guidelines, produced following a case study into cyber bullying.

Appendix B (PMS)

Code of conduct for use of the school computers and the internet

These rules apply at ALL times, in and out of school hours, whilst using school equipment.

Please read carefully:

- you must not download games or other programs from the internet.
- you must not use chat-lines or web-based email services (e.g. hotmail).
- you must not send, access or display offensive messages or pictures.
- you must not give your name, address, telephone number or any other information about yourself, or other people, to anyone you write to.
- you must not use or send bad language.
- you must not waste resources, particularly printing ink and paper.
- you should use print preview every time you send a document to the printer.
- you should only access websites that are appropriate for use in school.
- you should be careful what you say to others and how you say it.
- you should respect copyright and trademarks. (You cannot copy material without giving credit to the person or company that owns it.)
- you should check with a teacher before opening email attachments or completing on-line questionnaires or subscription forms.

PLEASE NOTE:

- User areas on the school network will be closely monitored and staff may review your files and communications.
- Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate.
- If applicable, external agencies may be involved, as certain activities may constitute a criminal offence.

Signature of pupil……..

Parent/Carer Signature ……

Date: ……

Signed document to be kept in the school planner and referred to prior to allowing students to access ICT network

Appendix C

Staff/Volunteer
School Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning . I will, where possible, educate the students in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

Appendix C

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has responsibility to provide safe and secure access to technologies and ensure the smooth running of the School.

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. Personal mobile devises are permitted to be used in school, when pupils are not present. Chargers and power supplies should not be used in school, unless they have been PAT tested by the school within the last 12 month ago.
- I will not use the school email system to send personal emails on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it will be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

Appendix C

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

E-mail & Internet Use Good Practice

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services.

You should:

- check your E-mail inbox for new messages regularly;
- treat E-mail as you would a letter, remember they can be forwarded / copied to others;
- check the message and think how the person may react to it before you send it;

- make sure you use correct and up to date E-mail addresses;
- file mail when you have dealt with it and delete any items that you do not need to keep;

You should not:

- use E-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- print out messages you receive unless you need a hard copy;
- send large file attachments to E-mails to many addressees;
- send an E-mail that the person who receives it may think is a waste of resources;
- use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

I understand that I am responsible for my actions in and out of the school.

- I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. In the event of illegal activities this would include the involvement of the police.

Staff / Volunteer Name:

Signed: Date