AVONMOUTH CHURCH OF ENGLAND PRIMARY SCHOOL AND NURSERY

E-safety and Acceptable Use of Technology

Date of Policy : October 2018

Review Date of Policy : October 2020

Contents:

Rationale:
In order to exploit the many educational and social benefits of new technologies, learners need opportunities to create, collaborate and explore in the digital world. At times they will encounter risks.

We recognise, however, that e-safety risks are posed more by behaviours and values online that the technology itself. Our approach must be to empower learners to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online, rather than restrict access to technology. Acceptable Use Policies, when embedded within a wider framework of e-safety measures, can help promote the positive behaviours needed. It is also imperative that the key principles of AUPs are shared with parents and carers to provide a shared expectation of the behaviour children must adopt whenever and wherever they are using technology.

Also contained in this document are AUPs for staff guidance, for data storage and security and use of school owned devices.

In writing this document, we have primarily considered recommendations from:

- *The Byron Review Report – "Safer children in a digital word" June, 2008;*
- *South West Grid for Learning;*
- *Becta – the government agency leading the drive to ensure the effective and innovative use of technology throughout learning;*
- *Bristol CYPS.*
- *RM Education*
- *The Prevent Duty- DfE June 2015*
- *Keeping Children Safe in Education – September 2016*

Roles and Responsibilities:
Protecting young people (and adults) properly means thinking beyond the traditional school environment. Access to the internet is not only available from the desktop computer, now many mobile phones, tablets, games consoles and other hand-held devices offer connections.

Pupils may be working online in places that do not have network protection such as is place at school. The emphasis therefore is for everyone to understand the risks and act accordingly.

This also means the involvement of a range of interests groups: Head Teacher; Governors; Senior Management; Class Teachers; Students; Support Staff; Pupils/carers; Parents; Local Authority Personnel; Community Groups and Volunteers who should also be made aware of the policies and practices in place regarding e-safety and acceptable use within our school.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist materials when accessing the internet in schools. School will ensure that suitable filtering is in place, however all staff should check materials from the internet before using them with children whenever possible and report any resource that causes concern.

E-safety and cyber bullying is a **child safety** issue.

Head Teacher and Senior Leaders:

The Education 's Inspectors Act 2006 empowers Headteachers to such an extent as is reasonable to regulate the behaviour of pupils 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Head Teacher:
- Is responsible for ensuring the safety, including e-safety of members of the school community (though day to day responsibility may be delegated);
- Have responsibility to ensure suitable CPD as relevant to e-safety;
- Will ensure that there is a system in place to allow for monitoring and support;
- Should be aware of procedures to be followed in the event of an e-safety incident or allegation of an e-safety event against a member of staff.

Governors:
Governors are responsible for approval of e-safety policy and reviewing effectiveness of the policy. A member of the governing body should take the role of e-safety governor and this role will include:

- Regular meetings with Head Teacher/e-safety officer;
- Monitoring of e-safety incident log;
- Regular monitoring of furthering control;
- Reporting the relevant Governor Committee.

Teaching and Support Staff:
Teaching and Support Staff are responsible for ensuring that:

- They have up to date awareness of e-safety matters and current school e-safety policy and procedures;
- They have read and signed the School Staff Acceptable Use Policy;
- They report any suspected misuse or problem to the Headteacher for investigation;
- Digital communication with pupils should only be on a professional level and carried out on school systems;
- E-safety issues are embedded in all aspects of the curriculum and other school activities;
- Pupils understand and follow school e-safety and AUP;
- They are aware of e-safety issues relating to the use of mobile phones, cameras and hand held devices, and monitor their use and implement such policies as appropriate;
- In lessons where internet use is planned, pupils should be guided to sites that have been pre-checked and that pupils are aware of procedures in place for dealing with unsuitable material found in searches.

Child Protection Officers and/or DSL/Deputy DSL with responsibility for e-safety:
The Child Protection Officers and/or DSL/Deputy DSL with responsibility for e-**safety** should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate online contact with adults/strangers;
- Potential or actual incidents of grooming;
- Cyber bullying.
- Radicalisation

These are child protection issues **not** technical issues. Technology provides an additional arena in which for child protection issues develop.

Pupils:
Pupils are responsible for using school ICT systems in accordance with the Pupil Acceptable Use Policy. Pupils need to:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- be expected to understand and know school policies on the use of mobile phones, cameras and hand held devices. They should understand school policies on the use of images and cyber-bullying;
- Understand the importance of e-safety when using digital technology outside of school and realise that the school e-safety policy covers their actions outside of school if related to their membership of the school.

Parents/Carers:
Parents/carers play a crucial role in ensuring their children understand the need to use the internet/mobile devices in an appropriate way. The school will take opportunities to help parents/carers to understand the issues through newsletters, the school website, and information sessions for parents etc.
Parents/carers should be:

- Responsible for endorsing the Pupil Acceptable Use Policy.
- Recognise their own role in making their children aware of e-safety issues and endeavour to ensure online safety for their children at home.

Community Users:
External agent users who access the schools ICT systems will be expected to read and sign the AUP for children and staff before being provided with access.

Policy Statements

Education – pupils

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

E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT/PSHE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside of school;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information;
- Pupils should be helped to understand the need for the student/pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Use of social media sites, texting & messaging requires particular attention in light of The Prevent Duty –June 2015
- Staff should act as good role models in their use of ICT, the internet and mobile devices and the use of social media.

Education – parents/carers

Many parents and carers have only a limited understanding of e-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 online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and when using social media sites and are often unsure about what they would do about it. "***There is a generational digital divide"*** (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, website;*
- *Parents evenings;*
- *Reference to the South West Grid for Learning Safe Website "Golden Rules" for parents and carers.*

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of e-safety training needs of all staff will be carried out regularly. It is expected that staff will identify e-safety as a training need within the performance management process;
- All staff will receive training in accordance with The Prevent Duty 2015, and are expected to be familiar with the content of the document.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies;
- The E-Safety Co-ordinator (or other nominated person) will receive regular updates through attendance at SWGfL/LA/other information/training sessions and by reviewing guidance documents released by BECTA/SWGfL/LA and others;
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days;
- The E-Safety Co-ordinator (or other nominated person) will provide advice/guidance/training as required to individuals as required.
- All staff will be required to sign the Acceptable Use Policy

Training – Governors

Governors should take part in e-safety training/awareness sessions with particular importance for those who are members of any sub committee/group involved in ICT/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation;
- Participation in school training/information sessions for staff or parents.
- Training and guidance in school, delivered by school staff.

Technical – infrastructure/equipment.

Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-safety Policy and guidance;
- There will be regular reviews and audits of the safety and security of school ICT systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school ICT systems;
- All users at Year 1 and above will be provided with a username by ICT subject leader, who will keep an up to date record of users and their usernames;

The school has provided enhanced user-level filtering through the use of the Bristol CYPS filtering programme. In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher / e-safety lead. Any sites accessed in this way must be used with caution and only by teaching staff. They must, not stored as short cuts on any device and should be closed immediately after use.

School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

Temporary access onto the school system will be agreed with the Headteacher and through separate access, including a secure password for the purposes.

The use of portable devices owned by the school is restricted to employees only and may only be taken off site with permission from a senior member of staff. All devices are signed in and out.

Staff are forbidden from installing programmes on school workstations/portable devices.

Downloading of files is only appropriate for school, not personal use. Permission should be sought from the technician for large files. Removable media (memory sticks/CDs/DVDs) must be kept secure at all times. Files stored in this way must be deleted after use. The school infrastructure and individual workstations are protected by up to date virus software.

Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Use of wireless broadband should be secured to at least WEP standard and must not be used off the school site without encryption.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned it is best practice that 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.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is acceptable 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 the Network Manager (via the Headteacher) 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.

Pupils 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.

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – Photographic, Video, mobile phones.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks.

All adults connected with school should be aware that images of themselves, posted online, or sent electronically to others, can affect the school's professional reputation or bring the school into disrepute.

When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, using, sharing, publication and distribution of images; in particular they should recognise the risks attached to publishing their own images on the internet eg. 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 should not be used for such purposes.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' 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 pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year.)

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its 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 eg. SIMs
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer systems, USB sticks or any other removable media:

- The data must be encrypted and password protected;
- The devices must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
- The devices must offer approved virus and malware checking software;

- The data must be securely deleted from the device in line with school policy (below) once it has been transferred or its use is completed.

Communications

A wide range of rapidly, developing communications technologies has the potential to enhance learning. However, we have considered the using of these technologies for education against the potential risks before making the following policy statements:

Staff and other adults

- mobile phones may be brought into school, but should not be brought out whilst children are present. They are only to be used in school offices and only during breaks, before & after school.
- taking photographs on mobile phones is not allowed;
- Use of school e-mail for personal e-mails, use of chat rooms/facilities, instant messaging or social networking sites is not allowed.

Pupils

- Mobile phones may be brought into school with staff permission and must be kept secure in the school office during the day;
- Pupils are not allowed to use their mobile phones for any purpose during the school day (this especially applies on school visits where it is important that phones remain in school).
- Use of the following is **not** allowed in school or on the school network:
  1. personal e-mail addresses;
  2. chat rooms/facilities;
  3. instant messaging (MSN);
  4. social networking sites.

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

- the official school e-mail service may be regarded as safe and secure and is monitored. (staff and pupils should therefore use only the school e-mail services to communicate with others when in school or on school systems (eg. By remote access);
- users need to be aware that e-mail communications may be monitored;
- users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail;
- any digital communication between staff and students/pupils or parents/carers (e-mail, chat, VLE etc) must be professional in tone and content;
- Pupils should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material;
- personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.
- All adults involved with school i.e teachers, govs,LSAs, admin/ premises staff SMSas, volunteers & students, must ensure that , if they use social networking sites or chat rooms, the professional reputation of the school relies on their own discretion, should not be called into question by anything posted.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sex abuse images;
- promotion or conduct of illegal acts. E.g. under the child protection, obscenity, computer misuse and fraud legislation;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist material in UK;
- pornography;
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;

- threatening behaviour, including promotion of physical, violence or mental harm;
- extremist and terrorist materials/media
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- using school systems to run a private business;
- use systems, applications, websites or other mechanisms to bypass the filtering or other safeguards employed by the school;
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords);
- creating or propagating computer viruses or other harmful files;
- carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in the use of the internet;
- On-line gaming (educational);
- On-line gaming (non educational)
- On-line gambling;
- On-line shopping/commerce;
- File Sharing;
- Use of social networking sites;
- Use of video broadcasting, without permission from the Deputy/Headteacher.

Responding to Incidents of Misuse

It is hoped that members of the school community will be responsible users of ICT, who will understand and follow this policy. However, there may be times when infringements of the policy could take place through carelessness or irresponsible or, very rarely, through deliberate misuse.

It is the responsibility of the Headteacher to respond to any apparent or actual incidents of misuse in the appropriate way. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

All incidents of misuse should therefore be reported to the Headteacher for investigation.

Incidents that raise a child protection concern should immediately be recorded and reported to a member of the Safeguarding Team.

Appendix 1

Avonmouth C. E. Primary School
Staff (and Volunteer) Acceptable Use Policy Agreement

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.
- That the professional reputation of the school remains intact.

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 students/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 and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people 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 system, e-mail and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg. Laptops, e-mail, VLE , cloud based systems, tablets and all mobile devices) out of school;
- I understand that the school ICT systems are primarily intended for educational use;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password (SIMs);
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person;
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and will respect the opinions of others.
- 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. Where these images are published on the school website it will not be possible to identify by name, or other personal information, those who are featured;
- I will only communicate with pupils 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 or the reputation of the school.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use personal hand held/external 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;

- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes;
- I will ensure that my data is regularly backed up, in accordance with relevant school policies;
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), covered by
- copy write, unlicensed , are 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.

When using the internet in my professional capacity or for school sanctioned personal 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).

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

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 out of school and my use of personal equipment in school 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. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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.

Staff/Volunteer Name …….

Signed …….

Date …….

Appendix 2

Avonmouth C. E. Primary School
Acceptable Use Policy – Pupils

- I will use the school's computers, IPads and internet connection for learning;
- I understand that I must use ICT systems in a responsible way;
- I may only use the internet when a teacher is present;
- I will ask permission before using the internet, and before entering a website not already approved by a teacher;
- I will not look at or delete other people's work or files;
- I will only use my own login;
- I will not use internet chat rooms;
- If I see anything I am unhappy about I will tell a teacher immediately;
- I know that the school may check my computer files and can monitor the internet sites I visit;
- I will never give out personal information or passwords;
- The messages I send will be polite and sensible.

Name of Pupil ……..

Name of Parent ……..

Date ……..

Appendix 3

Avonmouth C. E. Primary School

Sample letter to Parents/Carers

Dear Parent/Carer,

Re: Internet Permission Form

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students access to a large array of on-line educational resources that we believe can greatly enhance students' learning experience.

However, access to and use of the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's Acceptable Use Policy (enclosed). It is important that this enclosed document is real carefully, signed by a parent or carer and returned to the school.

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Yours sincerely,

Advice for parents is available from:
www. Parentsonline.gov.uk
South West Grid for Learning
BECTA