St George's C of E (V.A.) Primary School

Policy Document

E-Safety and E-Learning

E-Safety and E-Learning Policy

Version History

Version	Date	Comments
0a	22/10/2015	M Hewitt – First draft from previous policy.
0b	13/11/2015	M Hewitt – Updated following review.
0c	14/03/2017	M Hewitt – Updated.
1	18/07/2017	M Hewitt – Issued for use.

E-Safety and E-Learning Policy

Contents

E-Safety and E-Learning Policy

E-Safety and E-Learning Policy

Introduction

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 communication 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, as many new technologies can also present dangers for users.

Aims

This E-Learning Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour

Implementation

In order to meet these aims the school implements two main strands of action.

We will provide systems and implement procedures to reduce the possibility of exposure to illegal and disturbing material in the digital arena. However, we recognise that these can only be a backup to teaching children as these systems are never completely able to screen everything and children cannot be protected by school systems when outside of school. We will be particularly mindful where online safety impacts on our adherence to the following key documents:

- Keeping Children Safe in Education
- Children Missing in Education Guidance
- Female Genital Mutilation Multi-Agency Practice Guidelines
- The Prevent Duty

For this reason, our primary focus will be on educating the children in the use of technology. We will make them aware of the potential difficulties and dangers that exist in an online world and will teach them strategies to keep themselves, their friends and their families safe.

Acceptable Use

Three appendices to the document define acceptable use of the school's IT systems.

- Staff
- Key Stage 1 and Foundation Stage
- Key Stage 2

E-Safety and E-Learning Policy

All staff will be expected to sign their agreement before using the school's systems. Children and their parents will be encouraged to sign their agreement. As this is not possible to mandate, all children will be made aware of the agreement and expected to follow its principles whether signed or not.

E-Safety and E-Learning Policy

Technical E-Safety Policy

Introduction

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 ensure that relevant staff will receive guidance and training and will be effective in carrying out their responsibilities.

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school systems
- there is oversight from senior leaders and these have impact on policy and practice

Technical Security

- Appropriate security measures are in place to protect school systems from accidental or malicious attempts which may threaten the security of the school systems and data.
- The School Business Manager is responsible for ensuring that software license 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.
- All computers and devices in school should have access to the school's filtering systems.
- Any potential threats to safety or security should be reported to a member of Senior Management immediately.
- Records of all users and rights to be audited and kept by the School Business Manager.
- 'Guest' users should be provided with separate login details (e.g. students).
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious attacks.
- Any filtering issues should be reported immediately to the filtering provider.
- Changes to the filtering system should be checked and audited.
- Any websites that have been accessed that included inappropriate content should be logged and investigated and, if necessary, reported to the appropriate safeguarding institution.
- If staff bypass the filtering system by use of the password they must not permanently allow access to any sites.

Password Security

- All adults will be given their own username and password to access the school server. Children will also be given their own username and password.
- Passwords for new users, and replacement passwords for existing users will be allocated by the ICT coordinator.
- All users have clearly defined access rights to school systems. These include some non-school provided services (e.g. Cloud storage services (e.g. Dropbox), 3rd party educational services (e.g. EasyRead)).

- The administrator passwords for the school will be made available for technical staff, the head teacher and appointed senior leaders.
- Passwords should be different for different systems and must be secure.

E-Safety and E-Learning Policy

Responding to Incidents of Misuse

E-Safety Coordinator

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings and committee of Governors
- reports regularly to Senior Leadership Team

Online Safety Incident Procedure

In the event of suspicion, all steps in this procedure should be followed:

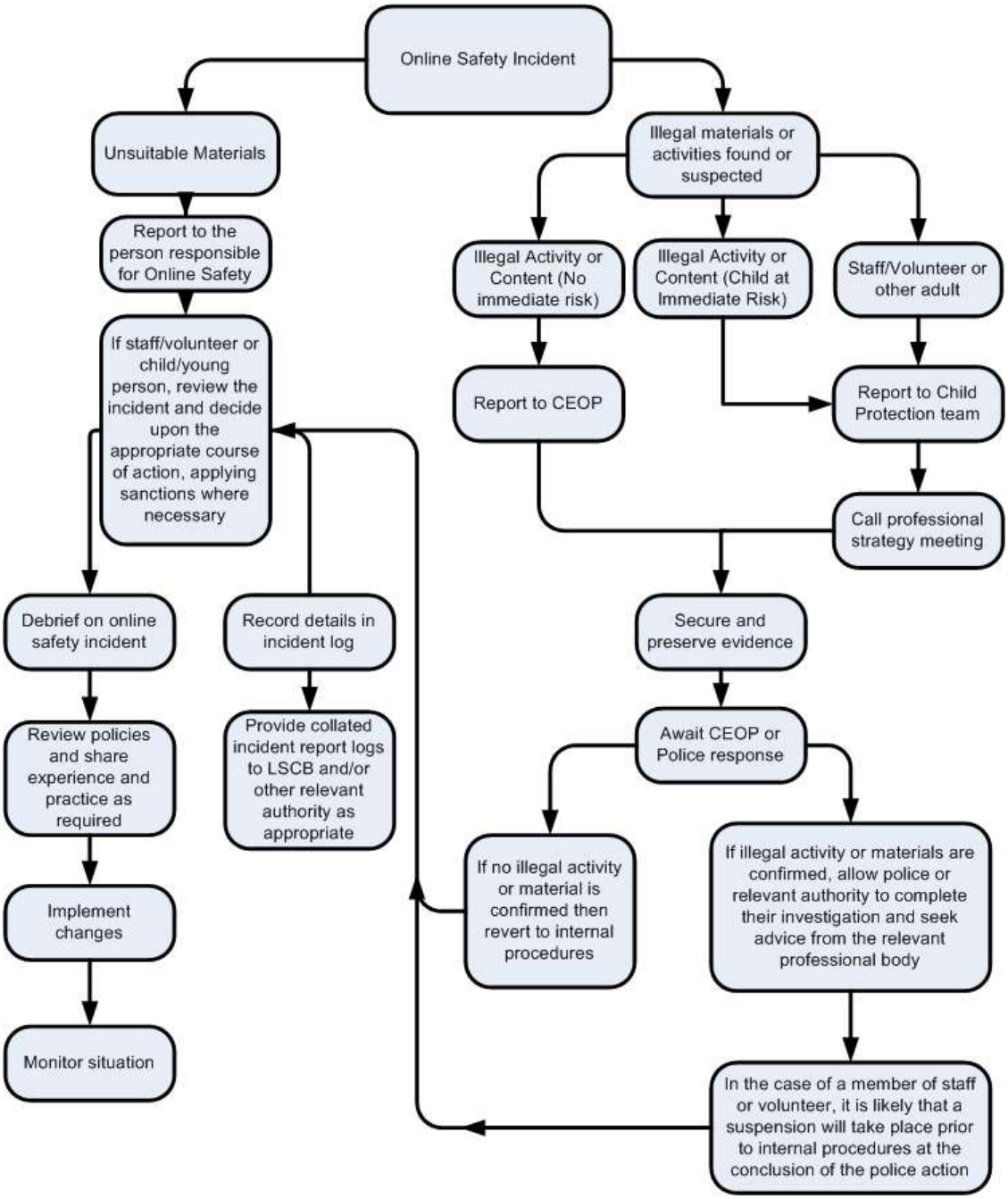
- Have more than one member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need 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 imagery of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge 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 (as relevant)
    - Police involvement and/or action

If content being reviewed includes imagery of child abuse then the monitoring should be 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

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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 purposes. The completed form should be retained by the group for evidence and reference purposes.



User Actions

Unacceptable and Illegal

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 sexual abuse imagery - the making, production or distribution of sexual imagery of children - contrary to The Protection of Children Act 1978
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003
- possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) - contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986

Unacceptable

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:

- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- terrorist and extremist material - in relation to the Prevent duty in the Counter-Terrorism and Security Act 2015

Users must not use school systems to:

- run a private business
- gamble on-line
- file share

Users must not:

- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- infringe copyright
- reveal or publicise confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- create or propagate computer viruses or other harmful files
- have unfair usage (downloading / uploading large files that hinders others in their use of the internet)

Acceptable for Nominated Users

- use of video broadcasting e.g. Youtube

Acceptable at Certain Times

- on-line gaming (educational)
- on-line shopping / commerce
- use of social media
- use of messaging apps

E-Safety and E-Learning Policy

Policy Review

This policy will be reviewed annually by the ICT coordinator and monitored by the head teacher.

Approval for Use

This Policy has been reviewed and ratified by the Governors on xxx – minute number - xxx

Approved -

Chair of Governors

Date -

E-Safety and E-Learning Policy

Appendix 1 - Staff Acceptable Use Agreement

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.

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 the use of school ICT systems (e.g. 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 not refer to students / pupils / parents / carers or school staff when using social media unless I have a genuine relationship with them outside of school.
- I will not engage in online discussion on personal matters relating to members of the school community.
- I understand that personal opinions should not be attributed to the school and should not bring the school into disrepute.

Professional Communication

- 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. I will appreciate that others may have different opinions.
- I will ensure that when I take and / or publish imagery of others I will do so in accordance with the school's policy on the use of digital / video imagery. I will not use my personal equipment to record imagery, unless I have permission to do so. Where children's imagery is published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. Photographs taken in school are the property of the school.
- I will never use chat and social networking on my own devices in working hours unless I am using it for educational purposes.
- I will only communicate with students / pupils and parents / carers using official school systems (unless I have a genuine relationship with them outside of school). 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 good name of the school.

E-Safety and E-Learning Policy

Bring Your Own Device

- All devices brought from home will be free from any inappropriate content.
- I will ensure that my devices are given to the network technician to ensure they use the school filtering system.
- Any device loss, theft, change of ownership will be reported to the ICT coordinator.
- Ensure that you have made all the appropriate measures to keep your device virus-free (e.g. install virus-software, choose a secure operating system etc.)

When using the internet in my professional capacity

- 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, videos, software).

Safe Use of Technology

- 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. Chargers should be PAT tested.
- 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 search.
- I will use school email addresses on the school ICT systems. In some cases my personal email will be used by agreement with the Headteacher.
- I will not open any hyperlinks in emails or any attachments to emails 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, in accordance with relevant school policies – see computer disaster recovery plan.
- I will not upload, download or access any materials which are illegal (child sexual abuse imagery, criminally racist material, adult pornography covered by the Obscene Publications Act) or any inappropriate material which 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 – if this happens or I inadvertently access inappropriate material then I will immediately report it to the network administrator and child protection officer.
- I will 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 unless agreed with the Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy.
- I understand that the data protection policy requires that any staff or student / pupil 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 the school policy to disclose such information to an appropriate authority (freedom of information policy).
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

E-Safety and E-Learning Policy

Use of digital and video imaging

- When using digital imagery, I will inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing imagery. In particular, they should recognise the risks attached to publishing their own imagery on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital imagery of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, this imagery should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video imagery.
- Staff and volunteers are allowed to take digital / video imagery to support educational aims, but must follow school policies concerning the sharing, distribution and publication of that imagery. Imagery should only be taken on school equipment, the personal equipment of staff should not be used for such purposes, unless express permission is given by the Headteacher – in which case all imagery should be transferred to school equipment and removed from personal equipment.
- Care should be taken when taking digital / video imagery that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with expectations of good practice in school.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

E-Safety and E-Learning Policy

Agreement

I understand that I am responsible for my actions in and out of the 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 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. This could include being given a warning. The matter may be referred to the Governors at the school for a decision on disciplinary action which may involve suspension or dismissal. The Local Authority may be involved, and in the event of illegal activities there will be the involvement of the police.

I have read and understand the E-Safety Policy 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 - KS1 and Foundation Stage Acceptable Use Agreement

This is how we stay safe when we use computers:

I will ask a teacher or adult in the class if I want to use the computers.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will always take care of the computers and other equipment (e.g. i-pads).

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me, or I think is wrong, on the screen.

I know that if I break the rules I might not be allowed to use a computer by myself.

Child's Name _____

Signed _____

Date _____

As the parent / carer of the above pupil, I will help my son / daughter understand these rules.

Name _____

Signed _____

Date _____

E-Safety and E-Learning Policy

Appendix 3 - KS2 Acceptable Use Agreement

Pupils should have an entitlement to safe internet access at all times. The school will ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Aims

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

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.

Personal Safety

- I understand that my school will monitor my use of ICT.
- I will be aware of 'stranger danger' when I am online.
- I will not give any personal information about myself or other when I am online (this could include names, addresses, email addresses, telephone numbers, age etc.)
- I will not send pictures of myself, of any kind, to anyone, unless it is directly supervised by an adult and is part of a planned activity to do with school e.g. educational links with another school.
- I will tell an adult in school if anyone tries to talk to me online.
- I will tell an adult immediately if I see anything unpleasant that makes me feel uncomfortable on the internet.
- When given a username and a password I will keep it safe and to myself.

Actions

- I will respect others' work and will not view, copy, remove or otherwise change any other user's files, without the owner's permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, unkind or bad language.
- I will not take or show imagery of anyone without their permission.
- I will not write, post or send anything nasty about anyone at our school. (This includes, emails, social networks and any form of mobile communication e.g. text messages – this includes doing any of these things outside school).

E-Safety and E-Learning Policy

Safe Use of Technology

- I will only use school devices for my school work, unless I have been given permission to by a teacher.
- I will not bring any personal devices in to school unless I have been given permission by a teacher. If I bring a phone in to school I will not use it and I will store it with an adult until the end of the day. I understand that if it is found in school it will be confiscated and my parents will be asked to come to collect it.
- I will not try to download or upload anything from the internet without permission.
- I will not use any social media at school unless it is part of a school activity.
- I will only use a computer or device when I have been told to or if I have asked an adults permission.
- I will ask permission to bring a USB memory stick into school and I will virus scan the memory stick before copying over any files.
- I will only visit websites that I have been told are safe. If I accidently come across any inappropriate websites or content on the internet, I will immediately tell an adult and will not show anyone else but them.
- I will only search for information that I have been told to by my teacher.

Agreement

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

I understand that the school also has the right to take action against me if I break any of the above rules, or if I take part in cyber bullying.

I understand that if I break any of the above rules then I am breaking the E-Safety agreement and I may be banned from the independent use of technology in school.

Child's Name _____

Signed _____

Date _____

As the parent / carer of the above pupil, I will help my son / daughter understand these rules.

Name _____

Signed _____

Date _____