St Margaret's C of E VA
Primary School

Safeguarding & ICT Policy

Ratified by Governing Body: October 2016

Review Date: October 2020

Safeguarding and ICT

Protecting young people in the online world means thinking beyond the school environment. As well as the computer to access the Internet, now many mobile phones and games consoles offer broadband connections.

Pupils may be working online in school, at home or in an Internet café. Increasingly students will have access to personal devices not covered by network protection and therefore the emphasis needs to be on educating all users as to the risks involved and their obligation to act responsibly while online.

All school staff should be aware of this policy and understand their personal responsibility with regard to keeping young people safe online and how to respond to e-safety incidents.

Safeguarding children and young people in both the real and virtual world is everyone's responsibility. It is an extension of general safeguarding and this policy should be read along side the Safeguarding and Child Protection Policy. The Head Teacher, supported by the governing body, will take the lead in embedding the agreed e-safety policies in practice.

The member of the Senior Management team with responsibility for safeguarding and should be the central contact point for all e-safety issues. All pupils should be made aware of the school's acceptable user policy and what to do if they have any Internet safeguarding concerns.

- 99% of children aged 8 – 17 access the internet (Ofcom, 2008)

- **Research shows that the Internet has led to more children and young people having access to some kinds of content that might not be appropriate for their age (e.g. sexual material)**

- Although children and young people are really confident using technology they don't always know how to judge what information they can trust and what they can't.

- Unwanted contact by strangers is also a problem and children are still meeting up with people they first met online, even when they know about the risks.

- Bullying can expand online, especially because it can be anonymous, and people feel less responsible for their contribution to the bullying.

- It can also be viewed again and again, by lots of people.

- Children and young people often upload things about themselves or others without necessarily understanding or thinking through what the long term effects might be. (Byron Report 2008)

Acceptable use policy

All schools should have an acceptable use policy. This should detail the ways staff; pupils and all network users (including parents) can and cannot use ICT facilities.

This should detail:

- System security
- Unauthorised activities
- Social Networking sites
- E-Mail
- Internet Access
- Laptops
- Resource Limits
- Privacy
- Sanctions
- Cameras including personal cameras
- Mobile phones

The Acceptable Use Policy should link with other safeguarding policies such as anti bullying, cyber bullying etc

All pupils in the school should be aware of potential risks and how to practise safe, responsible behaviour, wherever and whenever they are online.

Pupils should know where to seek help both in and out of school and how to report incidents. The children will be working towards their 'Byte Awards' achieved at the end of Reception Year 2, Year 4 and Year 6.

Pupils are not accountable for the actions that others may force upon them but there are sanctions that the school will impose if they act inappropriately when online.

Reporting Incidents

If a pupil receives an abusive e-mail or text they should report the matter to a member of staff as soon as possible. A copy of the e-mail with full headers, plus dates and times should be saved. Staff will investigate all complaints of abuse and take action accordingly.

Responsibility for handling incidents involving children will be taken by the Computing co-ordinator and the Designated Safeguarding Officer in consultation with the Head Teacher. If one or more pupils view inappropriate material the first priority will be to give them appropriate support. The pupil's parent'/carers will be informed and given an explanation of the course of action the school has taken.

If staff or pupils discover unsuitable sites, the Computing co-ordinator will report the URL (address) and contact to the ISP and the L.A. The filtering system used in all maintained schools in Somerset contains a mechanism for automatically reporting any attempts to access illegal sites on the Internet Watch Foundation list, to the Police. If it is thought that illegal material has been accessed outside of this filtering umbrella, after consultation with the Local Authority, the site will be referred to the Internet Watch Foundation (IWF) and the Police.

The school should provide guidelines for parents, carers and others on safe practice. The South West Grid for Learning in conjunction with the Avon and Somerset Police delivers a programme of parent's evenings. In Somerset, this is delivered to clusters of schools and every parent in Somerset has the opportunity to attend one of these meetings annually to keep up with the latest safety issues. The government have funded a DVD that informs parents of the issues and copies of this can be ordered by schools for distribution to parents.

Senior managers in schools are required to respond to a wide variety of e-safety incidents on a daily basis. The majority involve students, but on occasion it may be a teaching or non-teaching member of staff whose conduct is in question. Many of these incidents will be covered in the school's acceptable use

policy; where they are not, the Local Authority should be informed at the earliest opportunity so that appropriate action can be taken.

Age Restricted Material

Print publications are classified to provide information and protect people from viewing material that might be inappropriate or damaging to their moral and physical wellbeing. It is illegal to show, give or sell restricted materials to a person under the legal age. The Internet has little in the way of classification of materials, though several groups are attempting to introduce classification categories for describing web materials. Schools should ensure that processes are in place to minimise the risk of students gaining access to inappropriate materials, through supervision and monitoring. Blatant intentional exhibiting of age-restricted materials to pupils under the specified age is a serious breach of e-safety and may result in a criminal prosecution or suspension/dismissal
Any incident that involves inappropriate adult access to legal material should be dealt with by the school's discipline policy and the Local Authority should be informed of any action taken.

Any incident of racially motivated abuse via technology needs to be linked in with the monitoring of racial incidents in the school. Where an incident involves racial abuse, the Local Authority should be informed and they will decide whether or not Police involvement is required.

Incidents involving staff

Any incident involving a member of staff is a serious and often complex matter. There may be implications for the safety of pupils, fellow employees and the learning environment, and for the reputation of the school.

Harassment or grooming of another person using technology, or breaching their right to privacy, poses a serious threat to their physical and emotional safety, and may have legal consequences.

In all disciplinary instances, a school should consult with HR and must be careful to follow disciplinary protocols, ensuring that proper documentation and recording of information occurs and that appropriate counselling and support are given. Parents/carers of the pupil involved must be kept fully informed of the matter.

Depending on the incident the designated person and head teacher will decide on an appropriate course of action. This may include involving external agencies. The e-safety co-ordinator should review e-safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.

In the school context, very serious incidents tend to involve illegal materials, (particularly the viewing, possession, making and distribution of indecent images of children) or grooming, stalking or harassment facilitated by communication technologies.

Indecent images of children are defined under Section 7 or the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994) References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.

What to do in the event of discovery of illegal material

Discovery of illegal material within the school's network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by e-mail, because doing so will be an offence in itself. **If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off, as this could potentially compromise any evidence the device may contain**. Ideally incident specific advice should be sought VERY quickly, either from the Police or Southwest One ICT as soon as the incident becomes known. The advice given will be incident specific and will be different in each case, depending on the number of workstations involved or if the incident involves the entire network and fileserver.

Basic steps:

- **Seek immediate and specific advice from either Southwest One ICT or the Police, relevant to this incident.**
- **Prevent any further physical access to the device until the correct advice is gained.**
- **Unless absolutely necessary DO NOT remove the power from a working PC and definitely DO NOT start a PC if it is already turned off.**

- **Consider if it is necessary to prevent remote access to the device. If you suspect that a member of staff or pupil who has left the site, could remove or damage evidence on the device remotely, unplug ONLY the network cable from the back of the device to prevent this access from taking place.**
- **If the PC is already turned off, and it is no longer realistically possible to prevent further physical access to the device, (i.e. lack of supervision, high levels of access or an unoccupied location) disconnect the power at the base unit (not the wall) and remove the battery from a laptop. Store this device securely in a location where no one else can gain access to it and make a note of the date, time and name of the individual who performed this action.**

Under no circumstances should the e-safety co-ordinator, network manager or head teacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.