Covenant Christian School
e-Safety and Social Media Policy

Introduction
The internet is a great resource. It facilitates business and social interaction and is an valuable educational tool. It enables students to obtain knowledge on all kinds of subjects and to access packages specially designed to promote learning. It has become an integral part of family, work and social life and it is therefore important that schools use it and teach children to use it effectively.

However, as with so much of the science and technology that is available in a God-ordered world, it can be used for good or evil, so schools must teach their pupils how to use it safely and rightly for the benefit of themselves and others.

Safe Use of the Internet
Covenant Christian School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. It aims to protect children from the dangers of the internet by a combination of actions.

1) Staff will carefully select the websites they and the children will use. This will entail a prior check that the site does not contain unsuitable material or links to the same.
2) Unapproved software will not be allowed in students work areas and if found will be removed.
3) The school will take all reasonable action to prevent access to inappropriate material and to this end will use a filter across the whole school network. However, due to the nature of the internet and the rapid changes that can occur, it cannot guarantee that no such material will appear on a school.
4) Students will not have access to the use of any computer in the school unless they are being supervised by a member of staff.
5) Students will not be permitted to use social media sites (ie Facebook and Twitter) in school.
6) In line with the Portable Electronic Device Policy, students will not be permitted to use their own devices such as smart phones while on school premises. If such devices are brought into school they must be placed in the electronic devices box as soon as possible and collected at the end of the school day.
7) Children will be taught about the dangers of the internet and social media how to use them properly and safely. As soon as they are ready they will be advised as follows.
    a) As children they should never divulge personal details including their passwords, name, address, mobile and landline telephone number, email address and names of friends or family.
    b) They should understand the dangers of grooming. They should not meet any stranger they have been in touch with online without their parent's or carer's permission.

c) They should understand the dangers of placing personal photos on social networks or at any public place on the net where they can be identified in anyway e.g. through the photo's background.
d) They should appreciate the danger of logging on to sites which may lead them into bad behaviour including addiction and radicalisation.
e) They should report anything untoward they find on the net to their teacher or, if they are at home, to their parents or carers.
f) They should be made aware that they could be bullied through internet social media sites or emails and be advised to report such action to their parents, carers or teachers. Any instance of cyberbullying will be dealt with according to the school's Child Protection Policy. This includes Cyberbullying with regard to SEN, gender reassignment, religion, belief, race and disability,
g) They should understand that much of what is written or shown on the internet is incorrect and should be encouraged to check information they encounter on any website.
h) They should be trained in the correct use of copyright material including the need to acknowledge their sources. Illegal downloads of films and music are very common and these sites are sometimes linked to pornography, gambling and other unsuitable materials.
i) They should understand that it is possible to seriously damage their progress at school through misuse of the internet. They should not spend excessive time on social media, stay up late at night on the computer or leave their mobile phones on all night.

Students who misuse the internet will be disciplined according to the School Behaviour and Discipline Policy. They may have their account suspended. Their parent or carer may be informed. Misuse includes making changes to another pupils account and changing their password.

Staff e-Safety
Staff must be vigilant whenever they are supervising pupils on to the internet or on the internet themselves. Computers including laptops and tablets should be password protected and not be left on in a classroom such that pupils can have unsupervised access to websites. When using sites such as YouTube, staff must watch previously to check for suitability of language and pop ups.
Staff should not post pictures of children on the internet without parent's or carer's permission and should never attach children's names to pictures.
If staff discover any matter of concern on the internet, they should report it to the head of school. If it amounts to child abuse, the matter must be handled according to the Child Protection Policy. If it a criminal offence, it must be reported to the police.
Complaints of staff misuse or negligence must be referred to the head of school and dealt with according to the school's complaints policy.
Staff activities on the school internet must abide by the conditions of the Data Protection Act (1998) and the law on copyright.

Parents and e-Safety

In the school year, children will probably spend more time on the internet at home than at school so parents and carers have an important role to play in e-safety. They will be given a copy of this policy when their family joins the school, asked to note the methods the school is taking to keep children safe on the internet and as far as possible apply the same methods at home. In particular they will be asked to install e-safety software on their home computers if they have not already done so.

The attention of the parents will also be drawn to the advice given to children listed in sections (a) to (i) above especially to that which applies only to internet use at home such as the use of social media and emails.

Please also refer to the IT Policy, the Portable Electronic Devices Policy and the Electronic Presentation Material Policy.

December 2016 [1]