WHOLE SCHOOL POLICY ON
E-SAFETY AND CYBER BULLYING, including EYFS and After School Provision

1. **Introduction**

    1.1 *"Technology offers extraordinary opportunities for all of society including children and young people. The internet allows for global exploration which can also bring risks, often paralleling the offline world. Video gaming offers a range of exciting interactive experiences for children; however some of these are designed for adults. There is a generational divide between parents and children which means that many parents do not feel empowered to manage risks in the digital world in the same way that they do in the real world."* Dr Tanya Byron.

    1.2 e-Safety:*"the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate."* Ofsted.

2. **The role of technology in our pupils' lives**

    2.1 Technology plays an enormously important part in the lives of all young people. The increasing use of smart phones provides unlimited access to the internet, messaging, blogging (web logging), social media websites (like Twitter), video calls via web cameras built into computers, and phones (Skype), Wikis (collaborative web pages), chat rooms and other social networking sites (such as Facebook/Instagram), and to video sharing sites (such as YouTube).

    2.2 This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the School's role to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks; including cyber bullying, embarrassment, harassment, grooming, stalking, identity theft, and abuse.

3. **Keeping the School Network Safe**

    3.1 With the explosion in technology, the School recognises that blocking and barring sites is no longer adequate. We must teach all our pupils to understand the need to behave responsibly if they are to protect themselves. This is specifically the responsibility of the School's PSHE and Pastoral teams, including Junior/ Senior School teachers, Advisers, Personal Tutors and Heads of Year.

    3.2 The School's technical staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the School's software, hardware, and data. They monitor the use of the internet and emails and will report inappropriate usage to the Head of Year/SMT as appropriate.

    3.3 Certain sites are blocked by the School's filtering system and the School's IT department monitors pupils' use of the network. The IT department also monitors

email traffic and blocks SPAM and certain attachments. The School recognises that decisions about filtering are difficult, and can cause frustration for pupils and teachers (particularly when working on higher level research / examination work). We also acknowledge that pupils' use of their own mobile devices potentially allows unfiltered internet access which is beyond our control.

3.4　The School issues all pupils with their own personal School email address. Access is via personal LOGIN, which is password protected. The School gives guidance on the reasons for always logging off and for keeping all passwords securely. Passwords are personal, and logging onto another users account is a disciplinary matter. The School also has strong anti-virus protection on its network which is operated by the IT department.

4. **Treating Other Users with Respect**

4.1　The School expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the School's guidance on 'Respect for the Community' [copies of which are in the homework diary].

4.2　The School expects a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or mobile phone. The School's policy on educational visits explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, staff use School mobile phones (rather than their own); and pupil/staff phone numbers are deleted at the end of a visit.

4.3　Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School's approach to bullying is set out in the Whole School Anti-Bullying Policy. The School is strongly committed to promoting equal opportunities for all, regardless of race, religion, sex, sexual orientation or disability.

4.4　All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or other worrying issue to a member of the pastoral staff, such as their Junior School teacher/Adviser/Personal Tutor.

4.5　The use of mobile phones is guided by the School's Mobile Device Policy.

5. **ICT in the Curriculum**

5.1　All pupils are taught core ICT skills through the PSHE programme. ICT has transformed the entire process of teaching and learning at St Christopher. It is a crucial component of every academic subject and the majority of the School's classrooms are equipped with electronic whiteboards, projectors and computers. St Christopher has a number of ICT suites and pupils may use the machines there, and in the library, for private study. All of the school's boarding houses are equipped with computers and network points.

5.2　St Christopher recognises that internet safety is a child protection and general safeguarding issue.

5.3　Our PSHE and Pastoral teams have expertise in the safe use of the internet, and the dangers involved in the misuse of ICT. Through both the PSHE and Pastoral programmes, all year groups in the School are educated in the risks and the reasons why they need to behave responsibly online.

6. **Promoting the Safe Use of Technology**

6.1 The School's guidance is that pupils and staff should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

6.2 As well as PSHE and Pastoral programmes, the whole School takes part in the Anti-Bullying Week each year where E-Safety is a key factor.

6.3 Pupils of all ages are taught how to make use of the excellent online resources that are available from sites such as:

6.3.1 Safenetwork (www.safenetwork.org.uk)
6.3.2 Childnet (www.childnet.com)
6.3.3 Cyber Mentors (www.cybermentors.org.uk)
6.3.4 Cyber bullying (www.cyberbullying.org)
6.3.5 E-Victims (www.e-victims.org)
6.3.6 Bullying UK (www.bullying.co.uk)

6.4 Resources cover the many hazards encountered on the internet, and empower users with specific guidance, help and support.

7. **Involvement of Parents and Guardians**

7.1 St Christopher seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School. The School recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The School therefore advises parents about the potential hazards and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. This includes directing parents to appropriate sources of information and support, through the appropriate Junior School teacher, Adviser or Head of Year. The School website also has a link to external support agencies, and the School holds occasional information evenings for both Junior and Senior School parents and staff.

8. **Considerate Use of Electronic Equipment**

8.1 Mobile phones, smart phones, Ipads and other personal electronic devices should be switched off and stored securely during the School day, in line with the Mobile Device policy which is explained to pupils at the start of each academic year. They may be used during lunch-times, and in boarding houses after School.

8.2 Staff may confiscate personal equipment that is being used during the school day in contravention of the policy.

8.3 Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

9. **Misuse – Statement of Policy**

   9.1   St Christopher will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB (Local Safeguarding Children Board). If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

10. **Inappropriate Images appearing online**

   10.1   Children may be concerned that images of them (eg. those hacked from Snapchat) have been uploaded to public websites. It's really important that they are provided with support and know what to do if they lose control, particularly of a sexual image. It's never too late to get help.

   10.2   Talk to a counsellor at ChildLine on **0800 1111** or at www.childline.org.uk. ChildLine will also work with the Internet Watch Foundation to notify sites hosting images to have them removed.

   10.2   If young people are being harassed, threatened or blackmailed because of a sexual image they can report to us at CEOP via the CEOP report form at: www.ceop.police.uk/safety-centre

   10.3   If images end up on a site children can often report to the sites where they have been shared. Find out how to report to some popular sites in the 'Help' sections of our Thinkuknow for 11-13s & Thinkuknow for 14+ sites.

11. **Cyber Bullying**

   11.1   Cyber bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The School's Anti-Bullying Policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.

   11.2   Proper supervision of pupils plays an important part in creating a safe ICT environment at school but everyone needs to learn how to stay safe outside the school.

   11.3   St Christopher values all of its pupils equally. It is part of the ethos of St Christopher to promote considerate behaviour and to value diversity.

   11.4   Bullying and harassment in any form should always be reported. The children can do this using whichever method they feel most comfortable with:

   11.4.1   in person to any member of staff: Junior School teacher/Senior School Adviser/class teacher/Head of Year/School Nurse/Head of Upper or Lower Junior School/Head teacher.
   11.4.2   by email: *bullying@stchris.co.uk*
   11.4.3   to one of our trained VI Form Peer Mentors
   11.4.4   using the "Bullying Box" in the Senior School Library (which is checked daily by the Heads of Year)
   11.4.5   through Childline, whose phone number is in the Homework Diary.

11.5   It is never the victim's fault, and he or she should not be afraid to come forward.

12.   Staff Training:

12.1   A planned Safeguarding training session is provided as part of the induction programme for all new staff at the beginning of the academic year which includes e-safety advice.

12.2   Updates as part of Child Protection Training will be given as whole or part of group training.

12.3   Further guidance for staff can be found here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

Gavin Fraser-Williams
Director of Pastoral Care

Updated February 2018

FLOW CHART FOR RESPONDING TO INCIDENTS

Initial Disclosure

This could come from a pupil directly, a parent, a pupil's friend

Five points for Referral:

1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

Initial Review with Safeguarding Team

At this initial stage the safeguarding team review the information and consider the **five points for immediate referral**. They make an initial decision about whether the incident can be dealt with in house.

Police/Social Care/MASH referral

Refer to your local arrangements for dealing with incidents and contact local services.

Considerations – risk assessment

- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

Risk Assessment/Dealing with the incident

Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care.

Management in School

Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.