Trinity Christian School

Nursery, Primary & Secondary

TRINITY

CHRISTIAN SCHOOL

E-Safety Policy

E-Safety Policy

This Policy should be read in conjunction with other policies which include:

- Data Protection
- Mobile phone and other electronic devices
- Photographic evidence
- Child Protection and Safeguarding

We believe that:

- The internet provides instant access to a wealth of up to the minute information and resources from across the world, which would not ordinarily be available
- Virtual Learning Environments (VLEs) provide students with a platform for personalized and independent learning
- Provides students with up to date learning and factual information from around the world
- The internet and social net working sites enable students to research information outside of ordinary school hours and thus accelerate the potential for learning

We also believe that electronic learning:

- Equips students with the necessary skills that they need for future employment and other life skills

However we also recognise:

- Students might inadvertently access content of an unsavoury, distressing or offensive nature on the internet or receive distasteful or offensive electronic messages
- Students might receive unwanted or inappropriate emails from unknown senders or may be exposed to Cyber bullying
- Students may be groomed online and make themselves susceptible to abuse – this includes students being made the victim of extremist or radicalisation content

We believe that the advantages of the internet and electronic learning outweighs the risks involved so long as users are made aware of the issues and concerns and receive guidance and education in choosing and adopting safe practices and behaviour

Procedures for using PC's at Trinity Christian School:

- Students and all other users must access the network using their own logons and passwords. These must never be disclosed or shared.
- Users must respect confidentiality and attempts should never be made to access another persons individual folder on the network without permission to do so.
- Software should not be installed without prior permission from Mr Fisher (person responsible of managing the network working with Jim Towell).
- Machines must never be left logged on and left unattended. If machines are to be left unattended they should be locked (Ctrl+alt+del followed by lock computer) or logged off.
- Machines must be logged off after use and shut down at the end of school.
- All students from Y1 – Y11 must sign an E Safety User Agreement before given access to the internet.

- Parents and carers are required to sign a consent form before allowing students to use the internet
- The internet must only be accessed for professional or educational purposes (staff must not use the internet to access social networking sites, shopping sites or for other uses which is in connection with their private lives).
- Students must be supervised at all times while using the internet
- Rules and procedures for safe internet use must be clearly communicated with students and must be displayed in rooms with internet usage
- Accidental access to inappropriate sites (racist, abusive, pornographic or otherwise) must be reported to the teacher and a note will be taken of the offending site and blocked
- Internet and filtering software is installed at Trinity Christian School
- Internet activity will be monitored regularly by staff (Mr Fisher) and a half termly report given to the school's SMT and Governors
- Students and other users must never disclose personal details about themselves or others
- **Bullying, harassment or any kind of Cyber abuse will not be tolerated. Sanctions will be applied to the user who breaks this code (regardless of if the offence occurs outside of school hours or off school site)**
- If students or users are bullied or made to be victims of Cyber bullying they should report the offence to Mr. Stewart (designated School Lead) – and evidence kept of the abuse
- Antivirus software is installed and kept up to date at Trinity Christian School
- All users should seek permission from the teacher before down loading any files

Procedures for instant messaging:

- The use of instant messaging (MSN, Yahoo Messenger etc) is not permitted at Trinity Christian School

Procedures for the use of a camera at Trinity Christian School:

- Staff and students should use the designated school camera located in the School Office.
- Staff should download images on the day that images are taken or ask the Office Staff to do so.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Students must never upload images onto social networking sites (which includes tagging) without permission
- Parents must not take photos of other peoples children and should never upload photos on social networking sites (e.g. Facebook) without permission from the child's parents

Procedures for the use of mobile phones:

- Students are banned from using mobile phones. All students must hand their mobile phone to the Form teacher during morning registration. The phone will be returned during final afternoon registration

Mr. Andrew Fisher is the designated person for managing the computer system. In line with our dedication to ensure E-Safety he is required to make frequent checks to ensure that no material is being viewed by students and staff. Mr. Fisher will produce a half termly HEALTH CARE REPORT and make this available for SMT and Gov viewing. This report is in line with the schools Data Protection Policy

Mrs. Gemma Deakin is the designated person for managing the school webpage and Facebook page.

Mr Jim Towell is the designated person for maintaining our computer system from an external organization called Adoni software company.

Trinity Christian School offers a wireless network – to maintain e-safety this is encrypted and protected by a password. This password is only given to staff on a need to know basis and is **NEVER SHARED WITH PUPILS OR VISITORS TO THE SCHOOL** (including parents).

The practices and procedures in this Policy will be subjected to an annual review.

REVIEW: AUTUMN 2018

Appendix 1

Trinity Christian School
Bringing the Love of God into the Classroom

Primary Pupil Acceptable Use Agreement for E-safety

Dear Parent/ Carer

ICT including the Internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the School Office who will happily find out for you.

E-SAFETY RULES:

- I will only use ICT in school for school purposes.
- I will only use my class login and will not give it to anyone else nor use anyone else's.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my E-safety.

Please detach and return the slip to the School Office once read and understood (1 per child)

Primary E-Safety agreement

Parent/Carer declaration:
We/I have discussed this with ……………...…………………….........(child name)

They will endeavour to follow the E-safety rules and to support the safe use of ICT at Trinity Christian School.

Parent/ Carer Signature: …….……………...…………….....…………………………….

Print name/s:
....

Class/Year: ………………………………. Date: ………………………………

Trinity Christian School
Bringing the Love of God into the Classroom

Pupil & Parent E-Safety Home / School Agreement

PARENT DECLARATION (Y7-Y11 only)

Parent / Carer Name:

....

Pupil Name:

....

As the parent or carer of the above pupil, I grant my permission for my child to have access to the use of the Internet at school.

My child will sign this E-Safety agreement and they will have a copy of the 'Rules for Responsible ICT Use'.

I accept that ultimately the school cannot be held responsible for the nature and the content accessed throughout the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service and employing appropriate teaching practice and the teaching of e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / Carer signature:

.... Date:.............................

Appendix 2

<u>PUPIL DECLARATION (Y7-Y11 only)</u>

I agree to comply with the school rules for responsible ICT use (PTO).
If I break any of the rules for responsible ICT use this could lead to the following sanctions being enforced:-
1.   A temporary or permanent ban on Internet use.
2.   Additional disciplinary action in line with school's behaviour policy.
3.   Parents or guardian contacted.

PUPIL NAME: _____ Date: _____

Rules for Responsible ICT Use

1. I will only access the network using my own logons and passwords.
2. I will never share my logon and password with another person
3. I will never try to gain access to another persons electronic folder
4. I will never try to install software at school without asking permission from school to do so
5. I will never leave my computer unattended and will always log off when I finish my work
6. I will only use the computer and internet to access educational sites
7. I will never use the internet to access social networking sites such as Facebook
8. I will never access inappropriate sites such as racist, abusive, hate or pornographic sites
9. I will always tell a teacher if an inappropriate site comes up
10. I will never take part in any Cyber bullying activity – either at school or away from it
11. I will never delete any of my files without asking permission from the teacher
12. I will never save any materials without asking permission from the teachers

I understand that I will lose the privilege to use the internet if I break any of the above rules

I understand that the school will periodically check my files to ensure that I am abiding my the school E Safety rules