ST CHARLES' CATHOLIC PRIMARY SCHOOL

E-SAFETY/ ACCEPTABLE USER POLICY

E-SAFETY POLICY		
AGREED: MAY 2017	REVIEW: JUNE 2019	NEXT REVIEW: JUNE 2021

Our Mission at St Charles' Catholic Primary School is to…
LOVE, LEARN, GROW TOGETHER

St Charles' Catholic Primary School

E-safety/Acceptable User Policy

inc Social Media Policy

(use of mobile phones and digital photography)

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place inside and outside of school.

Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

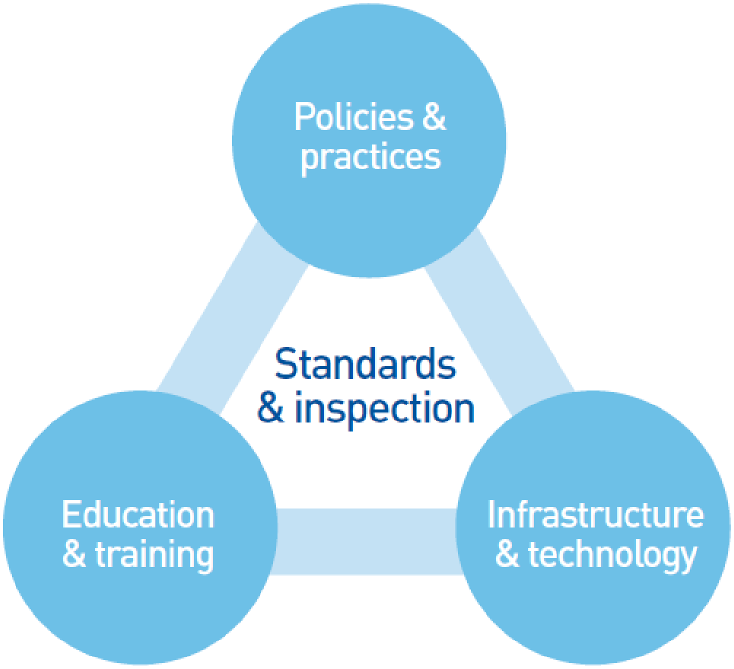
Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person, including technology addiction.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

The school have adopted the PIES model which is the basis of its approach towards E-Safety and helps to manage and minimise its risk.



Policies and practices
The e-Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the schools approach to E-Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to E-safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

Infrastructure and technology
The schools educational network and access to the internet is provided by Liverpool City Council through MGL. This network provides a safe and secure 10Mbps broadband connection to the internet. There is a multi-layer security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a cloud-based filtering service which filters internet content using the City Council's base

policy. The infrastructure has been designed to minimise the risk of: users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

Education and training
As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an E-safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potentially using and the risks that they potentially face.

Standards and inspection
The school reviews its approach to E-safety on a regular basis and uses the 360^o Safe tool to evaluate and improve its provision. Reference is also made to e-safety in the annual 175 audit and through Ofsted inspections.

Policy Statements

Whilst the PIES model forms the basis of the schools approach to E-safety the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the E-safety policy the school will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Unsuitable/inappropriate activities
- Incidents of misuse

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations Act 2018, which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure

- Only transferred to others with adequate protection.

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly “logged-off” at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the school ensures the following good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, on school business or on school systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

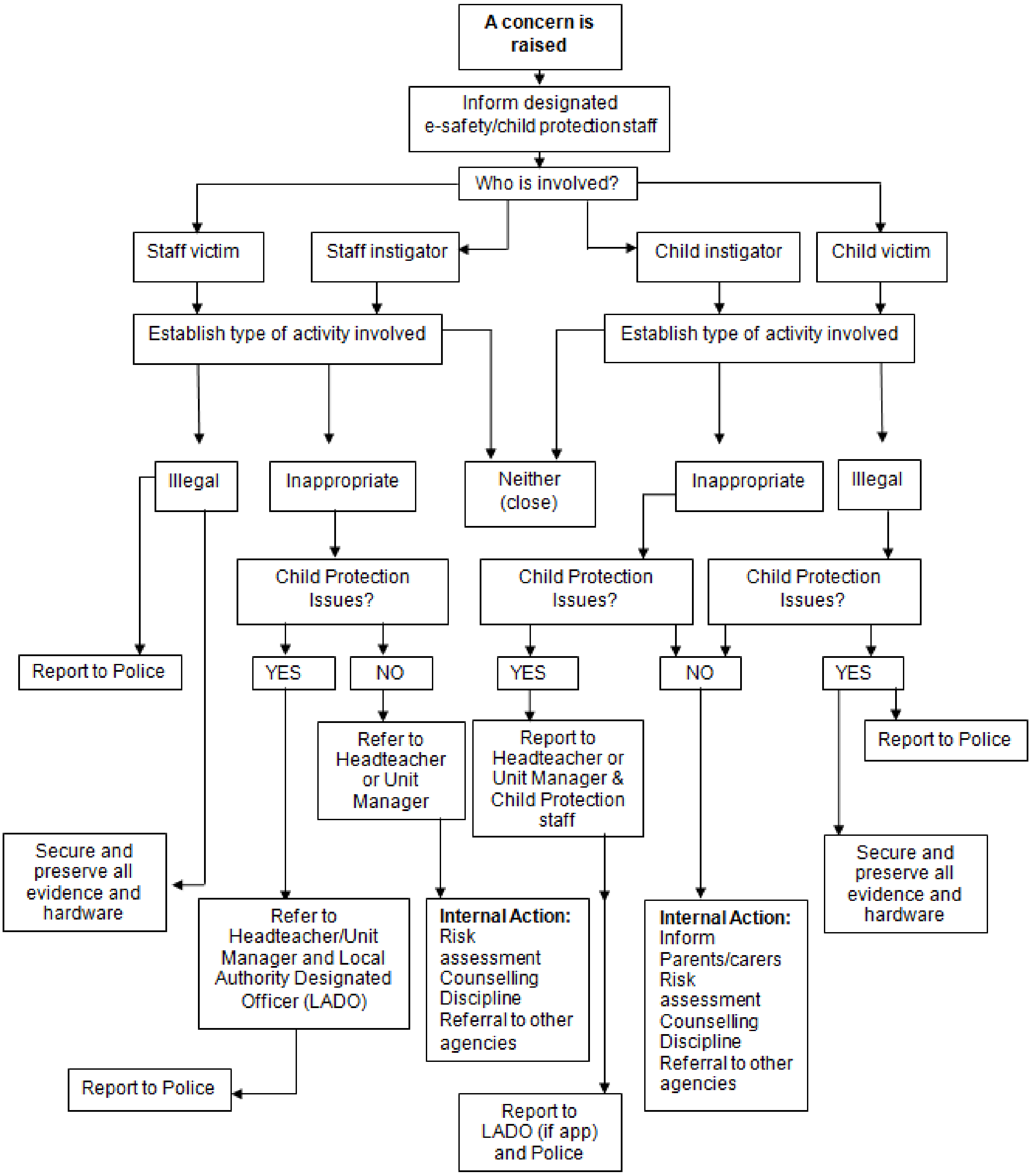
School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below.

All incidents will be recorded and reported to the relevant parties and organisations.


A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
YES
NO
YES
NO
YES
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
Report to Police
Secure and preserve all evidence and hardware
Refer to Headteacher/Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents/carers Risk assessment Counselling Discipline Referral to other agencies
Secure and preserve all evidence and hardware
Report to Police
Report to LADO (if app) and Police

Social Media Policy

Inc. use of Mobile Phones and Digital Photography

Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. This gives clarity to the way in which social media/mobile phones are to be used by pupils, social media/mobile phones are to be used by pupils, governors, visitors, parent helpers and school staff at St. Charles' Catholic Primary School. It will also provide guidance for parents.

There are four key areas:
A. The use of social networking sites by pupils within school
B. Use of social networking by staff in a personal capacity
C. Comments posted by parents/carers
D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school

The school's eSafety Policy outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate.

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff **must not** post information or opinions about St. Charles' Catholic Primary School or pictures of school events.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.

- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Behaviour and Discipline Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter. (Appendix 1)

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Head Teachers)

Use of Mobile Phones and Digital Photography Policy

Children are not allowed to have mobile phones in school. If children bring a phone to school they should take it to the school office where it will be kept until the end of the school day.

Children have their photographs taken to provide evidence of their achievements for their development records (The Early Years Foundation Stage, EYFS 2007).
Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.

Procedures

- Under the GDPR Act of 2018school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school network which is password protected until the school ceases to operate; should this occur then all photographs will be shredded or deleted from the school network.

- The school's digital cameras must not leave the school setting (unless on an educational visit).
- Photographs are printed in the setting by staff and images are then removed from the camera memory.
- Photographs of children may be taken and used in accordance with parental consent obtained annually
- Often photographs may contain other children in the background.
- Parents must not post photographs or video containing other children on social media websites. (See Policy above).

Appendix 1

Inappropriate Use of Social Networking Site

Dear Mr/Mrs……………..

It has come to the attention of the Governing Body that inappropriate comments regarding the school/members of the school community have been made on a social networking site.

As these comments do not comply with the expectations set out in the school's Social Networking Policy you are respectfully asked to remove them from the website.

We would encourage you to enter into productive communication with the school in order to resolve any outstanding differences. The school has an 'open door' policy with regard to dealing with parental communication and there are also policies in place such as the
Complaints Policy if required.

Yours sincerely

Chair of Governing Body