Sacred Heart Catholic Voluntary Academy

St Thomas Aquinas Catholic Multi-Academy Trust

E-SAFETY POLICY

Safeguarding is defined as protecting children from maltreatment, preventing impairment of health and/or development, ensuring that children grow up in the provision of safe and effective care and taking action to enable all children to have the best life chances.

Policy Date:	24/03/20		Kate Hayles Head Teacher	
Policy Review Date:	24/03/22		Edward Hayes Chair of Governors	Edward Hayes

Contents Page

Introduction	
What is E-Safety	3
Schedule for monitoring and review of Policy	4
Scope of Policy	4
Roles and responsibilities	
Policy statements	7
Education, Training & Infrastructure	
Data Protection & Communication	10
Communication usage table - staff and students	
Unsuitable/Inappropriate Activities and Table	11
Inappropriate use buy staff/students	
In the event of inappropriate use	
Illegal incidents and Flow Chart 1	14
Other incidents	16
Related Legislation	17
Useful Links - E Safety information and support	20
Appendix 1 - Secure transfer of data and access out of school	21
Appendix 2 - Acceptable Usage Agreement - Staff	22
Appendix 3 - Acceptable Usage Agreement – Student (Secondary Setting) – not applicable	26
Appendix 4 - Acceptable Usage Agreement – Students (Primary Setting)	27

Introduction

What is E-Safety?

Whilst the Internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young pupils. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school, it is our duty of care alongside that of staff/parents/carers and other members of the community to protect our children and young people from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures we take to ensure that pupils can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

Our school will endeavour to ensure the e-safety of all its members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this. Within our school, all members of staff and pupils are responsible for e-safety, responsibilities for each group include:

Students
Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.

- Complying with a highly visible pupil's rules for using the Internet that pupils must agree to each time they use the school's ICT equipment either in the school or remotely which connects to the Internet.
- Reporting any e-safety issue to the teacher, head of year, head teacher / principal or parent
- Taking responsibility for their own actions using the Internet and communications technologies.

All Staff
Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.

- Reporting any e-safety issues to the E-Safety Manager / Co-ordinator as soon as the issue is detected.
- Complying with a highly visible staff Acceptable Use Agreement (AUA) which staff must agree to each time they use the school's ICT equipment either in the school or remotely which connects to the Internet.

Teaching Staff
Educating pupils on e-safety through specific e-safety training sessions and re-enforcing this training in the day-to-day use of ICT in the classroom.

Network Manager/ICT Manager/ ICT Support Team
Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling pupils to use the Internet effectively in their learning.

- Ensuring that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Checking and auditing all systems to ensure that no inappropriate data is stored or is accessible
- Working with the E-Safety Manager / Co-ordinator to create, review and advise on e-safety and acceptable use policies
- Leading the development of the e-safety education programme for pupils and staff
- Managing a parental awareness programme for e-safety

- Dealing with e-safety breaches from reporting through to resolution in conjunction with the ICT support team
- Working with the ICT Team to create, review and advise on e-safety and acceptable use policies
- Working with outside agencies including the police where appropriate
- Maintaining a log of all e-safety issues
- Monitoring the technology systems which track student internet use to detect e-safety breaches
- Assisting in the resolution of e-safety issues with the E-Safety Manager / Co-ordinator and other members of staff

Schedule for Development/Monitoring/Review

The Governing Body approved this e-safety policy: ***November 2018***

Monitoring of the E-Safety Policy will take place at regular intervals.

The Governing Body will receive a report on the implementation of the E-Safety Policy.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date would be ***November 2019***

The school will monitor the impact of the policy using:

- Logs of reported incidents on Behaviour watch
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
- Pupils
- Parents/carers staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Sacred Heart CVA 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 out of school.

Roles and Responsibilities

The following section outlines in more depth the e-safety roles and responsibilities of individuals and groups within **Sacred Heart CVA.**

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Governors receiving regular information about e-safety incidents and monitoring reports will carry this out. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor / Director will include:

- Regular meetings with the E-Safety Manager / Co-ordinator/Designated Safeguarding Lead
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Manager/ Co-ordinator/ / Designated Safeguarding Lead
- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents – included in a later section – 'Responding to incidents of misuse' and relevant Local Authority HR / other relevant body disciplinary procedures, pages 17 & 18)
- The Head teacher/Senior Leadership Team are responsible for ensuring that the E-Safety Manager / Co-ordinator/ Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Head teacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Manager/ Co-ordinator/ Designated Safeguarding Lead

E-Safety Manager/ Co-ordinator/ Designated Safeguarding Lead

- Leads on e-safety issues
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority/relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meeting/committee of Governors
- Reports regularly to Senior Leadership Team

Network / ICT Manager

The Network Manager / ICT Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher/ E-Safety Manager/ Co-ordinator/ Designated Safeguarding Lead for investigation/action/sanction
- That monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (Appendix 2)
- They report any suspected misuse or problem to the Head teacher/E-Safety Manager / Co-ordinator/Designated Senior Person for investigation/action/sanction
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use agreements
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection/ Designated Safeguarding Lead

The Child Protection/ Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Accessing illegal/inappropriate materials
- Contacting inappropriate adults/strangers on-line
- Potential or actual incidents of grooming
- Cyber-bullying
- Peer on peer related incidents on and offline

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupils Acceptable Use Agreement (Appendix 3)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/ Virtual Learning Environment (VLE) and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/VLE and on-line student records (Where applicable)
- Their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems/website/VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Pupils

Keeping Children Safe in Education 2016, Annex C[1] describes e-safety as the safe and responsible use of technology. This includes the use of the Internet, and electronic media (eg text messages, gaming devices, email etc.). In practice, e-safety is as much about behaviour as it is electronic security. Use of technology has become a component of a number of safeguarding issues and e-safety in this context is classified into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT/PHSE/other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and offline and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children and young people visit

[1] **KCSIE 2016, Annex C**
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526153/Keeping_children_safe_in_education_guidance_from_5_September_2016.pdf

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Parents/Carers

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- The school website will provide e-safety information for the wider community

Education & Training – Staff/Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Manager / Co-ordinator/ Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school training/information

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed
- An agreed policy is in place for the provision of temporary access of 'guests' (eg trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department

Users may use the following types of removable media for the purposes detailed

- ✓ CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- ✓ USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- ✓ Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Bring Your Own Device (BYOD) – (Where applicable)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content
- Pupils must be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Further to this, the following table shows how our school currently considers using these technologies for education.

Communication Technologies	Staff & Other Adults				Students			
	Allowed	Allowed at certain times	Selected staff only	Not Allowed	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought into schools	✓				✓			
Use of mobile phones in lessons				✓	✓			
Use of mobile phones in social times	✓				✓			
Taking photos on (both school and non-school) mobile phones and other media devices				✓	✓			
Taking photos on school camera and media devices (projects/staff/students)	✓							✓
Use of other school mobile devices (tablets)(projects/staff/students)	✓							✓
Use of personal e mail address in school or on school network		✓			✓			
Use of school e mail for personal e mail				✓	✓			
Use of messaging apps (in school time)		✓			✓			
Use of social any media (in school time)		✓			✓			
Use of blogs (in school time)		✓			✓			

Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

	USER ACTIONS	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate, pass on, materials, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children, contrary to the Protection of Children Act 1978.					✓
	Grooming, incitement, arrangement or facilitation of sexual acts of children, contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008.					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation), contrary to the Public Order Act 1986.					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Any other information, which may be offensive to colleagues or breaches of the integrity of the ethos of the school or brings the school into disrepute.				✓	
Using school systems to run a private business					✓	

Using systems, application, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy/college				✓	
Infringing copyright				✓	
Revealing or publicising confidential or proprietary information (eg financial personal information, databases, computer / network access codes and passwords).				✓	
Creating or propagating computer viruses or other harmful files				✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet).				✓	
Online Gaming (educational)		✓			
Online Gaming (non-educational)				✓	
Online gambling				✓	
Online shopping/commerce				✓	
File sharing			✓		
Use of Social Media				✓	
Use of messaging apps				✓	

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk

School staff should ensure that

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority
- The school's use of social media for professional purposes will be checked regularly

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. When accessing the School's Learning Platform/Servers/Network from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the Event of Inappropriate Use

If a member of staff is believed to have misused the Internet or learning platform in an abusive or illegal manner, a report must be made to the Head teacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Pupil

Acceptable Use Agreements detail how pupils are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for pupils to understand what is expected of their behaviour and attitude when using the Internet.

This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to a fellow pupil, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School should encourage parents/carers to support the agreement. This can be demonstrated by signing the Acceptable Use Agreements together so that it is clear to the school that the pupil with the support of the parent/carer accepts the agreement. This is also intended to provide support and information to parents/carers when pupils may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

Should a pupil be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any pupil found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the pupil's use for a particular lesson or activity
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a pupil is deemed to have misused technology against another pupil or adult

In the event that a pupil accidentally accesses inappropriate materials the pupil should report this to a member of staff immediately and take appropriate action to hide the screen or close the window, so that the staff member can take the appropriate action. Where a pupil feels unable to disclose abuse, sexual requests or other misuses against

them to a member of staff, they can use the Report Abuse button (www.thinkuknow.co.uk)[2] to make a report and seek further advice. The establishment should also address the issue of a pupil deliberately misusing online technologies.

Pupils should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, as this may have legal implications.

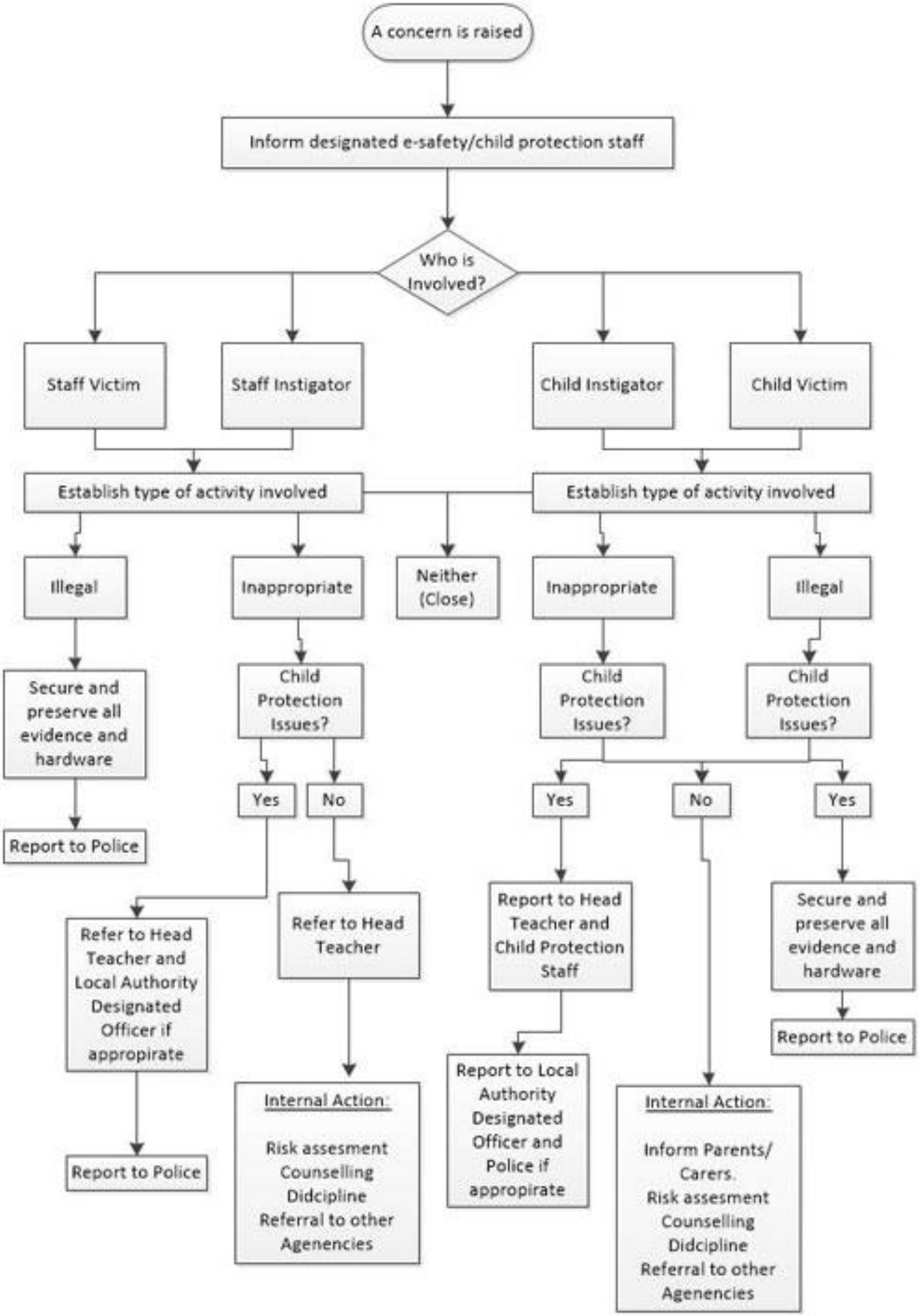
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of incidents. Incidents might involve illegal or inappropriate activities (See 'In the Event of Inappropriate Use' above). See flow chart(s) on the next page.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Flowchart(s) for responding to online safety incidents and report immediately to the police.

[2] http://www.ceop.police.uk/safety-centre/


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
Secure and preserve all evidence and hardware
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
Yes
No
Yes
No
Yes
Refer to Head Teacher and Local Authority Designated Officer if appropirate
Refer to Head Teacher
Report to Head Teacher and Child Protection Staff
Secure and preserve all evidence and hardware
Report to Police
Report to Police
Internal Action:
Risk assesment
Counselling
Didcipline
Referral to other Agenencies
Report to Local Authority Designated Officer and Police if appropirate
Internal Action:
Inform Parents/ Carers.
Risk assesment
Counselling
Didcipline
Referral to other Agenencies

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals of accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record the URL (Uniform Resource Locator) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant)
    - Police involvement and/or action
    - If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

        - incidents of 'grooming' behaviour
        - the sending of obscene materials to a child
        - adult material which potentially breaches the Obscene Publications Act
        - criminally racist material
        - other criminal conduct, activity or materials
        - isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

RELATED LEGISLATION

Legislation

Our school is aware of the legislative framework under which this E-Safety Policy and guidance has been written. It is important to note that in general terms, an action that is illegal if committed offline, is also illegal if committed online.

Where appropriate and when recommended, the school will ensure legal advice is sought in the event of an e-safety issue or situation.

Criminal Justice and Courts Act 2015
This new Act in brief investigates offences involving ill-treatment or willful neglect by a person providing health care or social care, looks at offences of disclosing private sexual photographs or films with intent to cause distress, offences of meeting a child following sexual grooming and possession of extreme pornographic images.

Section 33 in particular relations to disclosing private sexual photographs with intent to cause distress (Revenge Porn) and Section 37 looks further into meeting a child following sexual grooming.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Sexual Offences Act 2003
Meeting a child following sexual grooming S15 - The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer system;
- Obtain unauthorised access to a computer system with the intent of committing further crimes;
- 'Eavesdrop' on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material that is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material that is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (for DfE guidance:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444053/Searching_screening_confiscation_advice_Reviewed_July_2015.pdf

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems

Useful Links - E Safety information and support

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk
www.educateagainsthate.com
https://www.ceop.police.uk/
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Screening and confiscation
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Leicester Safeguarding Children's Board Procedures
http://llrscb.proceduresonline.com/chapters/p_ca_information.html

APPENDIX 1

Secure transfer of data and access out of school

Sacred Heart CVA recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe

Appendix 2

SACRED HEART CVA

ACCEPTABLE USE AGREEMENT (Staff/Volunteer) 2018/2019

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- SACRED HEART CVA ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That staff are protected from potential risk in their use of ICT in their everyday work

SACRED HEART CVA will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device in school. It applies across the whole network and includes Wi-Fi.

SACRED HEART CVA carries out secure content inspection. This means that when you access a site that uses techniques to secure the information between the website and yourself, SACRED HEART CVA can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

The school closely monitors your activity on the Internet; logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

The school email system is provided for educational purposes, where required the school has the ability to access your school email for safeguarding purposes.

Acceptable Use Agreement

I understand that I must use SACRED HEART CVA'S ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety

- I understand that SACRED HEART CVA will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to SACRED HEART CVA ICT systems (eg laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that SACRED HEART CVA ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using SACRED HEART CVA'S ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the SACRED HEART CVA website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

SACRED HEART CVA has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school's E-Safety Policy, Appendix 1. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of SACRED HEART CVA:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

Signed:_____

Name:_____

Date:_____

Appendix 3

ACCEPTABLE USE AGREEMENT

(Student)
2018/2019

Keeping safe: Stop, Think, before you Click!

- I have read the school's '13 rules for responsible ICT use'. My teacher has also explained them to me.

- I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

- This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.

- I understand that the school can check my computer files, and the Internet sites I visit and that if they have any concerns about my safety, that they may contact my parent / carer.

NAME	
SIGNARTURE	
DATE	

Keeping safe: Stop, Think, before you Click!
Our 13 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework
- I will only delete my own files
- I will not look at other people's files without their permission
- I will keep my logon and password secret and will not share it with other people including friends
- I will not bring files into school without permission
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school
- I will only e-mail people I know, or my teacher has approved
- The messages I send, or information I upload, will always be polite and sensible
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission
- I will never arrange to meet someone I have only ever previously met on the Internet or by e-mail or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me
- I will not use internet chat rooms
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it **but I will tell a teacher / responsible adult**

Version Control	
Author:	Julie Chapaneri & Mohammed Patel
Version:	1.2
Date:	1st August 2016
Review Date:	31st August 2017

Children, Young People & Families | Children's Safeguarding & Quality Assurance Unit
Bosworth House | Princess Road West | Leicester | LE1 6TH | T: 0116 454 2440 | E: safeguardingineducation@leicester.gov.uk