SACRED HEART

CATHOLIC VOLUNTARY ACADEMY

LIVE LEARN LOVE

E-SAFETY POLICY

APPROVED BY

THE GOVERNING BODY

NOVEMBER 2019 – NOVEMBER 2020

E-SAFETY POLICY

1. Introduction

1.1 Sacred Heart Catholic Voluntary Academy recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at Sacred Heart Catholic Voluntary Academy want to ensure that new technologies are used to:

- Raise standards;
- Develop the curriculum and make learning exciting and purposeful;
- Enable pupils to learn in a way that ensures their safety and security;
- Enhance and enrich their lives and understanding.

1.3 We are committed to providing learning experiences for all pupils using ICT technology.

1.4 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated senior persons for the implementation of the School's online safety policy are the Computing Coordinator and the Head Teacher who is also the Designated Child Protection Officer.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the school's facilities where they are used by voluntary, statutory or community organisations.

2.2 Sacred Heart Catholic Voluntary Academy will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- A range of policies including acceptable use policies that are frequently reviewed and updated;

- Information to parents that highlights safe practice for children and young people when using new technologies;
- Audit and training for all staff and volunteers;
- Close supervision of pupils when using new technologies;
- Education that is aimed at ensuring safe and responsible use of new technologies;
- A monitoring and reporting procedure for abuse and misuse.

3. Infrastructure and Technology

Partnership working

3.1 Sacred Heart Catholic Voluntary Academy recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the Schools' Broadband with Talk Straight who provide a managed (not 'locked down') network system. We fully support and will continue to work with Schools Broadband to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils, staff and families to assist us in developing our e-safety policies and procedures.

5. Use of new technologies

5.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

5.2 Sacred Heart Catholic Voluntary Academy expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below.[1] These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

---

1 For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, social media.

Users are not allowed to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

  Indecent images of children;
  Promoting discrimination of any kind;
  Promoting racial or religious hatred;
  Promoting illegal acts;
  Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e. cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material.

5.3 The school recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

5.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative);
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist or anti-religious material;
- Violence and bomb making;
- Illegal taking or promotion of drugs;
- Software piracy;
- Other criminal activity.

5.5 *In addition, users are not allowed to:*

- Use the Schools Broadband with Talk Straight or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves Schools Broadband with Talk Straight or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part School Broadband with Talk Straight or member Local Authorities or adversely impact on the image of Schools Broadband;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Schools Broadband with Talk Straight, or to Schools Broadband itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via Schools' Broadband with Talk Straight.
- Undertake activities with any of the following characteristics:
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the Schools' Broadband network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after Schools Broadband has requested that use cease because it is causing disruption to the correct functioning of Schools Broadband;
    - other misuse of the Schools' Broadband network, such as introduction of viruses.
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.
- 'Sexting' young people sharing sexual photographs or videos that they or another young person have created of themselves (DFE – Keeping Young Children Safe in Education).

5.6 Where Schools' Broadband with Talk Straight become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

6. The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.

7. Reporting Abuse

7.1 There will be occasions when either a pupil or an adult within the school receives an abusive message or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately (School log or follow Safeguarding procedures).

7.2 The school also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures assist and provide information and advice in support of child protection enquiries and criminal investigations.

8. Education and Training

8.1 Sacred Heart Catholic Voluntary Academy recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

8.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

8.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.
- Be aware of the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures.

9. Standards and Inspection

Sacred Heart Catholic Voluntary Academy recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

10. Monitoring

10.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use via adult supervision.

10.2 We will also monitor via adult supervision the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see Anti-Bullying Policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

11. Sanctions

11.1 We will support pupils and staff as necessary in the event of a policy breach.

11.2 Where there is inappropriate or illegal use of existing or new technologies, the following sanctions will be applied:

- *Child*
    - The child will be disciplined according to the Behaviour Policy of the school.
    - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- *Adult (Staff and Volunteers)*
    - The adult will be subject to the disciplinary process, if it is deemed he/she has breached the policy
    - Serious breaches will lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

11.3 If inappropriate material is accessed, users are required to immediately report this to the Head Teacher and Schools' Broadband with Talk Straight so this can be takern into account for monitoring purposes.

12. Working in Partnership with Parents and Carers

12.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

12.2 We also appreciate that there may be some parents who are concerned about the use of technology in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

12.3 Parents use of social media – Please refer to page 18 of Appendix 4 – Social Media Policy.

13. Appendices of the E-Safety Policy

13.1 Related aspects of the school's E-safety policy include Acceptable Use policies for both staff and pupils and Data Protection policy.

Review Date November 2020

Signed by 

APPENDIX 1 – ACCEPTABLE USE POLICY (ADULTS)

SACRED HEART CATHOLIC VOLUNTARY ACADEMY

STAFF AND VOLUNTEER ACCEPTABLE USE POLICY

School Policy

Technology has 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 technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This acceptable use policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- That school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Equipment

- When I use my personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), 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 when connecting these devices to school ICT systems, they are protected by up to date anti-virus software and are free from viruses.
- I will not install or attempt to install programmes of any type on school systems, 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 immediately report any damage or faults involving equipment or software, however this may have happened. Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check mobile equipment (e.g. iPads, laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also applies to use of school ICT systems out of school (e.g. laptops, email, social media etc).
- Use of external hard drives, memory sticks which contain school data **must be encrypted**.

Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.
- Unless I have permission, I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Email, chat, social networking and blogging

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- I will not use personal email addresses on the school ICT systems for school correspondence.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- I will only communicate with pupils and parents using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Use of mobile phones and digital images

- Mobile phones, personal cameras and recording devices should be stored securely during working hours on school premises or when on outings. (This includes visitors, volunteers and students)
- Mobile phones must not be used to take photographs in any teaching area in school or within toilet or changing areas
- Only school equipment should be used to record classroom activities. Photos should be put on the school system as soon as possible and not sent to or kept on personal devices
- All telephone contact with parents or carers must be made on the school phone and a note kept
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website, Class Dojo) it will not be possible to identify pupils by name, or other personal information.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy 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 out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: _____

Signed: _____ Date: _____

APPENDIX 2 – ACCEPTABLE USE POLICY (PUPILS)

SACRED HEART CATHOLIC VOLUNTARY ACADEMY

Acceptable Use Policy for Pupils

To keep me safe whenever I use the internet or email, I promise…

- to keep my usernames and passwords private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone or myself unless teacher led
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes or change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules…

I understand that the school's behaviour guidelines will be followed

I have read and understand this policy and agree to follow it.

Name of Pupil: _____

Signed: _____ Date: _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent's Signature: _____ Date: _____

APPENDIX 3 – Mobile Technologies

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.

The school allows:

	School Devices	**Personal Devices**		
	School owned for use by multiple users	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	No	Yes	Yes
Restricted network access	Yes	No	Yes	Yes
Internet only	Yes	No	Yes	Yes
No network access				

The school has provided technical solutions for the safe use of mobile technology for school devices -

- All school devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.

APPENDIX 4 – Social Media Policy

Social Media Policy

Contents

This policy is subject to Sacred Heart's Codes of Conduct and Acceptable Use Agreements. This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils (age restrictions followed) may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The school permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.**
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- **Parents/Carers**
    - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.