

SACRED HEART CATHOLIC VOLUNTARY ACADEMY

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 Primary School 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 an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give pupils with additional needs increased access to the curriculum to enhance their learning.

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 person for the implementation of the School's e-Safety policy is Mrs Karen Taylor.

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.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 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 East Midlands Broadband Community (embc) who provide a managed (not 'locked down') network system. We fully support and will continue to work with embc to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 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.

3.1.3 We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

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 and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

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

4.1.2 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.

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:

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, PDA's etc.

- 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.

4.1.3 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.

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

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

- Use the embc or an equivalent broadband provider's facilities for
- running a private business;
- Enter into any personal transaction that involves embc or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of embc or member Local Authorities or adversely impact on the image of embc;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of embc, or to embc 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 embc
- Undertake activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via the embc network and the effort of staff involved in support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the embc 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 embc has requested that use cease because it is causing disruption to the correct functioning of embc;
 - other misuse of the embc 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.

4.1.6 Where Synetrix (provider of Internet connectivity and associated services to

schools) and/or embc 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.

4.2 Reporting Abuse

4.2.1 There will be occasions when either a pupil or an adult within the school receives an abusive email 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.

4.2.2 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 LSCB² 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 Procedures³ assist and provide information and advice in support of child protection enquiries and criminal investigations.

² Chapter 9 of the LSCB Procedures

³ Chapters 5, 9, 12 and 13 of the LSCB Procedures

5. Education and Training

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

5.2 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.

5.3 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.
- Audit 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.

6. 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.

7. Working in Partnership with Parents and Carers

7.1 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.

7.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies 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.

Reviewed: September 2017