WRITTEN WITH GUIDANCE FROM LANCASHIRE SCHOOLS' ICT CENTRE.

Saint William's Catholic Primary School
Online Safety Policy
July 2021 – July 2023

Mission Statement

Alongside our families, parish and community, St William's will work together to ensure that each child will be taught as an individual.
We will help each child to reach their full potential through fun and engaging learning, in a safe, warm and caring environment.
We will teach them to live, love and learn in the way Jesus taught us.

"With God we are strong together, we can achieve together"

The implementation of this policy will be monitored by SLT and Subject Leaders and any other relevant staff.

Approved by Miss S Solloway (Head teacher) July 2021

Approved by Mrs J Clements (Chair of Governors) July 2021

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).
Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

This policy should be read in conjunction with other safeguarding policies and guidance.

2. Our school's vision for Online Safety

Our school provides a diverse, balanced and relevant approach to the use of technologies, especially as the children move further up the school.
Children are encouraged to maximise the benefits and opportunities that technology has to offer. As a whole staff we ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Children throughout school are aware of the rules for safe use of technology.
Following these rules ensures that children are equipped with the skills and knowledge to use technology appropriately and responsibly.

School does teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment in Computing, PSHE and assemblies.

All users in our school community understand why there is a need for an Online Safety Policy.

3. The role of the school's Online Safety Champion

Our Online Safety Champion is the Headteacher
The Online Safety Champion is the nominated point of contact within the school for Online Safety related issues and incidents. However, certain responsibilities may need to be delegated to other staff e.g. Subject leader or DSL/Backup DSL as necessary. The role of the Online Safety Champion should include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring any Online Safety Incident is logged.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools Computing Team and website and through advice given by the Safeguarding Team.
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person (if this is not the same member of staff) to ensure a co-ordinated approach across relevant safeguarding areas.

4. Security and data management

In line with the requirements of GDPR (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data is:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are regularly informed and reminded as to what they

can/cannot do with data through the Online Safety policy and statements in the Acceptable Use Policy (AUP).
All staff with access to personal data understand their legal responsibilities. They understand that they should only use approved means to access, store and dispose of confidential data.
Electronic data is stored on computers in the Headteacher's office and school office.
These computers are not accessible from elsewhere in school and are password protected.
Systems to access data e.g. Sims are also password protected.

Only the Headteacher has remote access to school data. This is accessed through a secure wireless facility and is password protected.
The school does not currently use "Cloud" Storage facilities apart from those provided through BT Lancs (office 365). This satisfies requirements of the Data Protection Act.
Staff laptops are allowed to be removed from school premises. These are password protected.
School data is backed up through BT Lancs (office system).

5. Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of Online Safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- That some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered Internet content. Pupils therefore are not allowed unsupervised access to any mobile device and must not bring their personal devices to use in school.
- That any devices used outside of school are virus checked before use on school systems.

Mobile telephones

In our school the following statements outline what we consider to be acceptable and unacceptable use of mobile phones.
Mobile phones are not permitted in school for children's use unless they travel to or from school without an adult. Any brought to school will be stored in the office or the teacher's secure stockroom until the end of the day.
Staff should ensure their own phones are turned off/silent and not used in the classroom when there are children present. The school office will take emergency calls and information passed to the relevant member of staff. Sending text messages and making phone calls should, wherever possible, be avoided in classrooms.

This policy also applies to visitors.
Mobile phones must never be used in toilet or changing areas.
It is acceptable to use personal mobile phones for school activities e.g. school trips.

Pen drives

Children are not permitted to bring pen drives into school. Where staff use these devices, they should be virus checked before information is transferred to the school system.
Images should only be taken with school cameras/iPads.

Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools

with challenges particularly regarding posting or sharing media in the Internet through mobile technologies and Social Network sites.

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), school must have written permission for their use from the individual and/or their parents or carers.
Permission is obtained from parents/ carers as part of the induction process. Clear information is provided about the taking and use of images, for within school and for other uses e.g. website, media. A list of pupils who have not got parental consent for these images is circulated to the appropriate school staff.
Sometimes children's photographs are used for press purposes. All parents sign to give permission for photographs to be published in the press. A list is kept of any children who do not have permission for this.
Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
Children's first name and surname will never be used on the website with a photo of just one child and where possible child photos will be bunched together.
Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs, but are asked not to publish them online or on personal websites where anyone can view them.
All staff recognise and understand the risks associated with publishing images and know that no images should be posted on social network sites. Staff should only use school equipment to take images related to school and should never use mobile phones for this purpose. They should not store digital content on personal equipment.
When taking images, staff ensure that subjects are appropriately dresses and not participating in activities which could be misinterpreted.
Images taken must be transferred as soon as possible to the secure school drive and removed from any mobile device. Photos taken in school must not be taken out of school on mobile devices.

Communication technologies

The school uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

In our school the following statements reflect our practice in the use of email.
Staff at Saint William's have access to the Lancashire Grid for Learning service. Our Computing subject technician or head is able to set up new accounts for both staff and pupils.
Only official email addresses should be used to contact staff and parents/ carers
The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts but users still need to be aware of the risks of accessing content from external email accounts.

All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
All users, both staff and/or pupils, must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Network sites

Social Network sites allow users to be part of a virtual community. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.
NB: LCC safeguarding guidance is shared with staff.

Many Social Network sites have age restrictions for membership e.g. Facebook's minimum age is 13 years old.
All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils and parents must never be added as 'friends' on any Social Network site.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Instant Messaging:

This is a popular tool used by adults and pupils that allows 'real time' communication and often integrates the ability to transmit images via a webcam. Although these sites are 'blocked' for use in Lancashire schools by default, some exceptions are made, see video conferencing.
Sites will stay blocked unless use of the site is part of a planned unit of work. The site will then be temporarily unblocked by the Headteacher, for the duration of the lesson. Pupils will be supervised at all times.
Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts through-safety lessons/training.

Websites and other online publications

The school website provides an effective way to communicate information.
Everyone in the school is made aware of the guidance for the use of digital media on the website.
Mrs H Hogarth, Mrs M Davis and the Headteacher are allowed to edit the website.
It is made clear there are to be no pictures linked to full names.
Content is always considered subject to copyright/personal intellectual copyright restrictions.
Documents on the website are in PDF format.
Others:
As we risk assess and introduce new technologies we will need to update our policy to reflect what we consider to be acceptable and unacceptable use of these.

Acceptable Use Policy (AUP)

The school has an Acceptable Use Policy to ensure that all users of technology within school will be responsible and stay safe. Adherence to the policy ensures that all users are protected from potential risks in their everyday use of technology for educational, personal and recreational purposes.

AUPs are signed by staff, pupils and guests and are signed by users before access to technology is

allowed. It forms part of our partnership agreement between parents, carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

The school's AUP:

- Is relevant to the setting and purpose.
- Is written to be easily understood by each individual user.
- Is regularly communicated to all users, particularly when changes are made to the Online Policy/ AUP
- Outlines acceptable and unacceptable behaviour when using technologies, including; Cyberbullying; inappropriate use of email, communication technologies and Social Network sites and any online content, acceptable behaviour when using school equipment/ accessing the school network.
- Outlines the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provides advice for users on how to report any failings in technical safeguards.
- Clearly defines how monitoring of network activity and online communications will take place and how this will be enforced.
- Outlines sanctions for unacceptable use and makes all users aware of the sanctions.
- Stresses the importance of Online Safety education and its practical implementation.
- Highlights the importance of parents/ carers reading and discussing the content of the AUP with their child.

Dealing with incidents

Even when procedures are followed there may occasionally be incidents related to Online Safety. An incident log should always be completed to record and monitor incidents.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF).
We will never personally investigate, interfere with or share evidence as we may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details can be found at www.iwf.org.uk

Inappropriate use

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence.
Some examples of inappropriate incidents are listed below with suggested sanctions.

<table>
<tr><td>Incident</td><td>Procedure and sanctions</td></tr>
<tr><td>Accidental access to inappropriate materials</td><td>Minimise the webpage/ turn the monitor off

Tell a trusted adult

Enter the details in the Incident log and report to LGFL filtering services if necessary

Persistent “accidental” offenders may need further disciplinary action</td></tr>
<tr><td>Using other people’s logins and passwords maliciously</td><td rowspan="4">Inform Headteacher or ICT coordinator

Enter details in Incident log

Additional awareness raising of Online issues and the AUP with individual child/ class/ adult

More serious persistent offences may result in further disciplinary action in line with the Behaviour Policy.

Consider parent/ carer involvement</td></tr>
<tr><td>Deliberate searching for inappropriate materials</td></tr>
<tr><td>Bringing inappropriate electronic files from home</td></tr>
<tr><td>Using chats and forums in an inappropriate way</td></tr>
</table>

The Headteacher, Senior Leader or Computing Subject Leader are responsible for dealing with Online Safety incidents. Pupils are informed of procedures as part of Online Safety learning. Guidance on the safe use of Computing and technology is displayed in the classrooms.

6. Infrastructure and technology

As a school, we are responsible for ensuring that our infrastructure/network are as safe and secure as possible.
The school subscribes to the Lancashire Grid for Learning and Broadband Service. Therefore, internet content filtering is provided by default. The Netsweeper filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school’s subscription and it is installed on computers in school and configured to receive regular updates.

Pupil Access

Pupils can only log onto pre-set areas of the network. Pupils are supervised when accessing school equipment and online materials.

Passwords

Staff have access to secure areas and have individual usernames and passwords.
Administrator passwords are kept securely.
Staff and pupils are reminded of the importance of keeping passwords secure.

Software/hardware

Our IT technician regularly update computers and check hardware.
The school has legal ownership of all software.
Appropriate licenses are up to date.
A regular audit of Computing equipment and software is carried out.
The Computing Subject leader controls what software is installed on school systems.

Managing the network and technical support

BT is the current Lancs provider of technology support for the office.
The school also buys into technical support from a local IT company. The technician ensures all systems are kept up to date with critical software updates and patches.
The technical support providers are aware of school requirements/ standards regarding Online Safety.

The Headteacher and Computing Subject Leader are responsible for liaising with the technical support staff.
Staff and pupils are required to log out of a computer when it is left unattended.
Pupils are not allowed to download executable files or install software.
Users should report any suspicion or evidence of a breach of security to the Computing Subject Leader (Mrs Hogarth) or the Headteacher.
Removable storage devices should only be used by school staff and this should only be when absolutely necessary.
ICT equipment should not be removed from the school, with the exception of staff laptops or portable recording devices e.g. iPad. Teachers' laptops should not be used by family members and should only be used for school purposes.

7. Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.
Education and training are essential components of effective Online Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online guidance must be embedded within the curriculum and advantage taken of new opportunities to promote Online Safety.

Online across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own Online Safety. Our school provides suitable Online Safety education to all pupils.

- Regular, planned Online Safety teaching is provided. This is differentiated for age and ability.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues. The school has a culture of telling.
- The pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

- We ensure that pupils develop an understanding of the importance of the Acceptable Use Policy and we encourage them to adopt safe and responsible use of IT both within and outside school.
- Pupils are reminded of Online Safety use by displays, signs, rules.

Online – Raising staff awareness

The Acceptable Use Policy is regularly reviewed and discussed as part of staff training.
Online training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social network sites.
All staff are expected to promote and model responsible use of IT and digital resources.
Online information is included in the staff handbook and induction procedures. This ensures that all staff fully understand the school's Online Safety Policy and Acceptable Use Policy.

Online – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school offers regular opportunities for parents/carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies.
Parents are given the opportunity to speak to teachers who can give appropriate advice where appropriate.
There is some promotion of external agencies advice on our website, which will need to be regularly checked for relevance.

Online – Raising Governors' awareness

The Headteacher is responsible for ensuring that Governors, particularly those with specific responsibilities for Online Safety, Computing or Safeguarding, are kept up to date. This will be through discussion at Governor meetings and appropriate training.

Standards and inspection

- The school will keep a log of any Online incidents- this will allow us to monitor the impact of Online Safety policies and procedures.
- The Headteacher and Computing lead are responsible for monitoring, recording and reviewing incidents.
- Any incidents will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children. Appropriate action can then be taken e.g. working with a specific group, class assemblies, reminders for parents.
- Monitoring and reporting of Online Safety incidents will contribute to changes in policy and practice, where appropriate.
- This policy and AUPs will be reviewed every two years.

Next review date; July 2023

S.Solloway