St. Francis Xavier's RC Primary School

Love one another as I have loved you

Online Safety Policy

Our Mission

Share God's love with one another

Follow your dreams

E**x**cel in citizenship

Our Mission is to:

- Be a witness to the values, teaching and beliefs of the Roman Catholic Church
- Promote achievement and enjoyment for all
- Expect the best for individuals
- Inspire learning
- Collaborate with the community
- Promote a healthy and safe life style
- Create a sustainable school
- Continually strive to be effective

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. Technology is transforming the way that schools teach and that children learn, particular with the introduction to home learning in light of Covid-19. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

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

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school's e-safeguarding policy has been written from a template provided by Herefordshire Council's Learning and Achievement Service which has itself been derived from that provided by the Southwest Grid for Learning.

Section A - Policy and leadership

Responsibilities: e-safety coordinator

Our e-safety coordinator is the headteacher for the day-to-day issues relating to e-safety. The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with school IT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- attends relevant meetings and committees of the Governing Body
- receives appropriate training and support to fulfil their role effectively
- The headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, through day to day responsibility.

Responsibilities: governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. Mrs D Hillyer is the safeguarding governor, and her role involves:

- regular meetings with the e-safety co-ordinator

Responsibilities: classroom-based 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 report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with pupils should be on a professional level and only carried out using official school systems or Seesaw blog. Please refer to social media policy.
- e-safety issues are embedded in the curriculum and other school activities.
- shortcomings in the infrastructure are reported to the computing coordinator or head teacher so that appropriate action may be taken.

Policy Scope

This policy applies to all members of the school community including staff, pupils, volunteers, parents, carers, and visitors.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Should a serious e-safety incident take place the headteacher will contact the West Midlands Safeguarding Children's Board, the Herefordshire Police and CEOP.

The school follows the Prevent Duty guidance from the DfE published in 2015 and last updated in March 2024.

Acceptable Use Policy (AUP)
All members of the school community are responsible for using the school IT systems in accordance with the acceptable use policy, which they will be expected to sign. Acceptable use policies are provided for:

- Pupils (EYFS + KS1 / KS2)
- Staff
- Parents and carers (including permissions to use pupil images, work and use of IT systems)

Acceptable use policies are signed by all children and parents and carers as they enter school and at the start of KS1. The signed document is stored in the class folder and handed over each academic year to the child's new teacher.

The Acceptable Use Policy is revisited annually and amended accordingly in the light of new developments. Discussions with the children take place at the time. Staff sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes a variety of permissions. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

The Induction Policy for school employees makes reference to the AUP.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core IT / computing policies

Computing Policy	How computing / technology is used, managed, resourced and supported in our school
E-Security Policy	How we categorise, store and transfer sensitive and personal data. This links strongly and overlaps with this e-safety policy.

Other policies relating to e-safety

Anti-bullying	How our school strives to eliminate bullying – link to cyber bullying
PSHE	E-Safety has links to this – staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy
Behaviour	Linking to positive strategies for encouraging e-safety and resulting sanctions if disregarded.

Illegal or inappropriate activities and related sanctions
The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable on IT kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Herefordshire Council or St Francis Xavier's School
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial or personal information, databases, computer or network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites or profiles for non-educational purposes

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

The examination of the data or files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Guidance for protection of personal information

Sensitive information relating to pupils' personal information should only be sent using Anycomms+.

School information being sent regarding pupils should be password protected.

Staff must ensure that they do not use school ICT equipment for personal use, e.g. cameras or computers.

Staff must keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.

Staff must never share their work logins or passwords with other people.

Staff must not give their personal e-mail addresses to pupils or parents. Where there is a need to contact parents, staff email addresses should be used.

Staff must keep a record or their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.

Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Seesaw and Tapestry class pages are kept private and password protected.

Use of Technology and Communication between pupils and school staff

Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

This includes the wider use of technology such as mobile phones, text messaging, e-mails digital cameras, videos, web-cams, websites and blogs.

Where appropriate, the school will provide a work e-mail address for communication between staff and pupils

Staff must not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

Staff must ensure that all communications are transparent and open to scrutiny. They must also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

Staff must not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

Social Contact

Staff must not establish or seek to establish social contact via social media or other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher or member of staff are part of the same social circle. These contacts, however, will be easily recognised and openly acknowledged.

There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

School Owned devices allocated to members of staff

- Personal IDs (often with associated personal media collections, eg music from iTunes) are not to be used on school owned devices.
- It is not permissible for children to have access to staff tablets unless very carefully supervised.
- A passcode is used on dedicated staff devices.
- All data is removed from tablets before it is allocated to a different member of staff.
- Individual teachers are responsible for ensuring that any data, apps or photographs stored on the iPad or computer are appropriate and professional. This is particularly important when mirroring to interactive whiteboards and screens.
- Members of staff must report immediately any loss or compromise of the device or data contained.

Personally owned staff devices

- Members of staff are permitted to bring their personal mobile devices into school.
- Members of staff are free to use these devices in school, outside teaching time for lesson planning purposes.
- Any staff mobile technology brought into school must be protected with a PIN code.
- Members of staff will not use their personal phone or tablet for taking photographs or capturing video of children.
- Mobile phones must be set to silent while in school (this applies to visitors as well as staff employed by the school).
- The school is not responsible for the security of personally owned technology.

School Owned devices used by pupils

- Mini laptops are available for children to use in school
- iPads are managed by John Finch Computers.
- Age-appropriate apps are purchased and deployed with due regard to licensing and copyright.

Personally owned pupil devices

We recognise that the area of mobile technology is rapidly advancing, and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Pupils are not permitted to bring mobile phones or any personal device into school.

Use of communication technologies

Email

Access to school email is provided for all users in school via Office 365 accessible via the web browser from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg: by remote access).
- Users need to be aware that email communications will be monitored
- Pupils, where appropriate, can communicate with the class using the Seesaw blog with the permission and guidance of their class teacher.
- E-safety education is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Any digital communication between staff and pupils, pupils and parents or carers must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social networking (including blogging)

- Teachers are encouraged to use educationally sound social networking tools, e.g. blogging, with children
- Only approved tools are used (Tapestry in EYFS and Seesaw in KS1 and KS2).
- The use of non-educational and age-inappropriate social networking by children is forbidden.

Use of digital images (still and video)

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- 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.
- In accordance with guidance from the Information Commissioner's Office, parents and 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 or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other pupils in the digital images.
- It is our school's policy to include a note to this effect on programmes for school performances and events.

Use of web-based publication tools

Website

Our school uses our website for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses (ideally as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Photographs or video published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs

Cloud based systems

Class teachers monitor the use of cloud-based systems by pupils regularly in all areas, but with particular regard to messaging and communication.
Pupils are advised on acceptable conduct and use when using the learning platform.
Only members of the current pupil, parent/carers and staff will have accounts.
When staff or pupils leave the school their account or rights to specific school areas will be disabled.

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive
b) The material will be removed by a member of staff if the user does not comply
c) Access to the system for the user may be suspended
d) A pupil's parent/carer may be informed

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE Teachers' standards - GOV.UK . Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content.

- These communications may only take place on official school systems.
- Staff members are not permitted to have pupils, or ex-pupils (under the age of 18) as friends when personally using social networking sites.
- Staff members are strongly advised not to have parents as friends when personally using social networking sites.
- Staff members must not post comments / images / opinions that relate to school life.

Our whole school community constantly monitors and evaluates developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

Section B Infrastructure

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Our school buys broadband services from John Finch Computers and we automatically receive the benefits of a managed filtering service using recommended software.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinator** in conjunction with John Finch. As well as John Finch the school has the ability and control over the web filter to allow or block websites at their discretion.

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Policy

The school has a filtering and monitoring policy in accordance with the DFE guidelines. This ensures that both the staff and students are protected from the many dangers online. John Finch approved software automatically implements a default filtering policy which prevents access to the most commonly blocked web categories. It is also compliant with the Prevent duty document.

Technical Security and Personal Data Security and Transfer

Please refer to the school's ***E-security Policy***.

Section C. Education

E-safety education

Whilst regulation and technical solutions are very important, they use must be balanced by educating pupils 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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of Computing, PHSE and other lessons. This is also reinforced during computing lessons.
- Online safety discussion prompts are used at the beginning on Computing lessons to promote staying safe online
- Learning opportunities for e-safety are built into the Herefordshire Primary Computing Progression where appropriate and are used by teachers to inform teaching plans.
- Key e-safety messages are reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils are encouraged to adopt safe and responsible use of technology within and outside school.
- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites pupils visit.
- Teachers should pre-plan websites which are suitable for open-ended research projects
- Adults to promote the use of Kiddle (children's' search engine) for finding information online

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address)
    - Cross checking references (can they find the same information on other sites)
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- We teach children, using 'Teach Computing' and daily internet safety when using online devices, about the four main areas of risk: content, contact, conduct and commerce.
- Pupils are taught how to make best use of recommended internet search engines to arrive at the information they require and to be aware of fraudulent or ill-informed content. Children are regularly alerted to the dangers of scams, conspiracy theories and disinformation and misinformation.

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates, and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology could be helpful in their learning.

Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- The school constantly monitors staff training needs and e-safety training is cascaded from the e-safety co-ordinator and available via Hoople CPD on-line at Herefordshire Council and safeguarding meetings
- All new staff should ensure that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- Staff Insets features regular E-safety updates in line with current events and developments in e-safety.
- The e-safety co-ordinator receives regular updates through her role as DSL, attendance at training sessions, Herefordshire DSL network meetings, the media, DfE documentation, Ofsted Engagement Hub, NSPCC website, net-aware, the local authority Spotlight circular, parents and the West Midlands Safeguarding Board
- The e-safety co-ordinator will provide advice, guidance and training to individuals, as required, on an on-going basis.

Governor training

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in IT, e-safety, health and safety or child protection. This may be offered in several ways:

- Attendance at training provided by the local authority, national or local governors association or other bodies.
- Participation in school training and information sessions for staff or parents

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences.

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

- Letters, newsletter (SWAY) updates- Wake Up Wednesday leaflets from The National College
- Parents' evenings and workshops

This policy was updated in September 2025. The policy was adopted by the Standards and Curriculum Committee of the Governing Body of St Francis Xavier's RC Primary on 29.9.25. This policy will be monitored and reviewed every two years.

Signed: Mrs S Cockroft	Date:29.9.25	Chair of Standards and Curriculum Committee
Signed: E Christopherson	Date:29.9.25	Headteacher
Signed: Adam Tunna	Date:29.9.25	Computing Subject Lead

Elizabeth Christopherson 29.9.25
Headteacher

Adam Tunna 29.9.25
Computing Subject Lead