St Norbert's Catholic School

Technology Safety Policy and acceptable usage documents

Date Adopted: Lent 2020
Date of Review: Lent 2022

ST. NORBERT'S
CATHOLIC PRIMARY SCHOOL

Our Mission Statement
St. Norbert's strives to nurture and develop the whole child through a
Love of God
Love of one another
Love of life itself

Article 17

You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to incorporate the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Web-based applications
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs/ Vlogs
- Podcasting
- Video/TV Broadcasting
- Music Downloading
- Gaming
- Mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. We understand the responsibility to educate our pupils on Esafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe, respectful and legal when using the internet and related technologies, in and beyond the context of the classroom.

When considering online safety, the 3 Cs for online safety are used as a benchmark for determining appropriate online behaviours.
(source www.internetmatters.org)

The 3Cs of online safety

Content – Is what I am seeing appropriate for me?
Contact – Is what this person saying to me safe?
Conduct – Am I behaving in a safe and respectful way?

Some of the potential dangers of using technology may include:

- 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 such as 'fake news'.
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Being at risk of computer viruses and hacking.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, cameras etc.); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

End to End E-Safety

E-Safety depends on effective practice at a number of levels:
• Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and acceptable usage agreements.
• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

• Safe and secure broadband Network including the effective management of LEA / CMAT preferred filtering product.
• Use of National Education Network E-Safety and UK Safer Internet Centre standards and specifications based on their current research and findings.
Access at: https://nen.gov.uk/ and

https://www.saferinternet.org.uk/

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named E-Safety Coordinator in our school is Miss **India Whyles** and the designated safeguarding Officer is **Mrs Jenna Withers**. All members of the school community have been made aware of who holds these posts. It is the role of the E-Safety Coordinator and designated Safeguarding Officer to keep abreast of current issues and guidance through organisations such as Lincolnshire LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leaders and Governors are updated by the Headteacher or E-Safety Coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding, health and safety, home–school agreements, and behaviour (including the anti-bullying) policy and PHSE.

Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an ICT curriculum that incorporates E-safety that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information (Parent pocket guides) and training opportunities for parents and carers to raise their awareness of the technologies that their children are potentially using and the risks that they may face.

E-Safety skills development for staff

- Our staff receive regular information and training on E-Safety and Safeguarding issues.
- Details of the ongoing staff training programme can be found in the CPD record.
- New staff receive information on the ICT Policy, Technology safety and Safeguarding policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.
- Relevant updates and areas to be aware of are regarding e-safety are circulated by the Headteacher and/or the ICT leader.

Managing the school E-Safety messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Technology policy- e safety messages will be introduced to the pupils at the start of each school year.
- E-safety areas within class will be prominently displayed.
- The central ICT suite will have a central display themed around an e-safety message.
- Pertinent messages and updates for parents are shared via Twitter and the school newsletter.

E-Safety in the Curriculum

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online (cyber) bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member or an organisation such as Childline/CEOP report abuse button.
- Internet use will always be supervised and permission obtained.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Each year children will take part in Internet Safety Day and Anti-Bullying Week to ensure they understand the importance of e-safety and are kept up to date with the changes in technologies.
- Each year the children will take part in Anti-Bullying week which has a special focus area on cyber-bullying.
- Pupils will be taught how to report content they come across in school or at home that they are unsure about or deem inappropriate.

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Technology Policy.
- Users are provided with an individual network, email and log-in username.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Headteacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unsupervised and are locked.

Data Security

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data.

- They must not allow others to view the data
- They must not edit the data unless specifically requested to do so by the Headteacher.
- If staff are taking data off site it will be password protected.

- Staff personal devices such as laptops, tablets, phones are not to be used in school for photographs, video and other forms of creating data relating to children or school.
- Staff are up to date with GDPR requirements and CMAT policy
- Children do not have access to areas of the server deemed sensitive as are staff. The admin area for example is also not available for pupils nor is it visible for staff due to data sensitivity.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the St. Norbert's Internet Web Filtering Systems is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by the Lincolnshire Safeguarding Children Board (LSCB) E-Safety Officer through its e-Safety responsibilities.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Safe 'child friendly search engines or tag words (eg: KS2, for kids) will be encouraged
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher or specific links directly provided. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Senior staff and ICT governor will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Virus protection will be updated regularly.
- School internet access is managed by our ICT supplier using Netsweeper and internationally renowned filtering service.

- The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the page/site must be closed and the incident reported immediately to the E-Safety Coordinator.
- The E-Safety Coordinator will contact the relevant network host company to remove access to links for the unsuitable site

E-mail

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. All email interaction within school and communication (including chat facilities) as part of school provided learning platforms will be closely monitored.

- The school gives all staff their own email account to use for all school business. This is to minimize the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Attachments will be virus checked through the school security system.
- Pupils are introduced to email as part of Computing KS2 National Curriculum and clear instructions of conduct are made explicit.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff must inform (the E-Safety Coordinator/line manager) if they receive an offensive e-mail.
- E-mail sent to an external organisation should be written carefully and authorised by a teacher or Head teacher before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters this includes jokes and funny statements. is not permitted in school or on school provided learning platforms.

Published content and the school web site and Twitter

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The advice for using photographs on a website is no different from their use in any other kind of publication or publicity material. However, the staff and governors of St Norbert's School are aware of the potential risk of inappropriate use of images because of the lack of control over who might see the image and the wide extent of the misuse of the Internet by certain people. The governors will seek the consent of parents regarding the use of images on the Internet and on Twitter. Children's surnames will not be included in photographs of children published on the school website. It is the responsibility of the Class Teacher to ensure only children with website and Twitter permission are used on published images.

The Press

The use of photographs in newspapers and magazines is already subject to strict guidelines. The Press Complaints Commission's Code of Practice states that:

- Journalists must not interview or photograph a child under the age of 16 on subjects involving the welfare of the child in the absence of or without the consent of a parent or other adult who is responsible for the children.
- Pupils must not be approached or photographed while at school without the permission of the school authorities.
- There is no breach of GDPR in passing on a child's name to a journalist as long as parental consent has been secured.

St Norbert's School will provide names of children to accompany photographs published in newspapers and magazines only where the parent or guardian have provided their consent.

Filming Events

Photographs and videos of children at school events such as the annual Nativity Play and Sports Day are not permitted. Any objections to this policy should be addressed to the Headteacher. The governors of St Norbert's School will seek the consent of parents/guardians regarding the use of photographs/film of children at these events. On occasions, commercial video films may be made of children on educational visits and performing in school productions. The school will inform parents where arrangements have been made for a commercial photographer to film such an event.

Where a commercial photographer is used, the school will follow the NSPCC (2019) guidelines which are as follows:

- ensuring the photographer wears identification at all times
- informing children, their parents and carers that a photographer will be at the event and ensuring they consent to images which feature their child being taken and shared
- not allowing the photographer to have unsupervised access to children
- not allowing the photographer to carry out sessions outside the event or at a child's home
- reporting concerns regarding inappropriate or intrusive photography following our child protection procedures.

Source: https://learning.nspcc.org.uk/research-resources/briefings/photography-sharing-images-guidance/

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as tablets, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging and existing technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

These devices should be PIN protected or locked using the relevant device method.

- Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school. If phones are needed for after school if walking home alone, they must be handed into the office before school and picked up at the end of the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Images, videos and sound recordings of children made on personal devices are not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact pupils outside normal school hours.

School provided Mobile devices (including phones)

The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and Tablets for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school and should be password protected. No other person should be accessing the teacher laptop when off site.

The Safe Use of Children's Photographs

Schools need and welcome publicity. Children's photographs add colour, life and interest to articles promoting school activities and initiatives. Making use of photographs for publicity materials and to promote the school in the press can increase pupil motivation and staff morale, and help parents and the local community identify and celebrate the school's achievements. However, photographs must be used in a responsible way. Schools need to respect children's and parents' rights of privacy and be aware of potential child protection issues.

At St Norbert's School every reasonable effort will be made to minimise risk by following the guidelines detailed in this document and by securing parental consent for the use of photographs.

St Norbert's School will not display images of pupils or staff on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school have access. Where photographs are taken at an event attended by large crowds, this is regarded as a public area so it is not necessary to get permission of everyone in a crowd shot.

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school Twitter feed
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' surnames names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching and support staff and pupils within the confines of the school network
- Portable storage containing school specific information (data, photographs etc.) that is taken off the school site is to be password encrypted.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school will keep a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.

- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed by the IT governor, the ICT/e-safety leader and Head Teacher.
- Any relevant information pertinent to safeguarding for these emerging and trending technologies will be circulated to staff and parents where appropriate.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Complaints

Complaints relating to E-Safety should be made to the E-Safety Coordinator, Designated Safeguarding Lead/Headteacher. Incidents should be logged. Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures. Pupils and parents will be informed of the complaints procedure. Advice would be sought from LEA in the event the school needed to establish procedures for handling potentially illegal issues.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety Coordinator/ Designated Safeguarding Lead/HeadTeacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Coordinator, depending on the seriousness of the offence; investigation by the Headteacher/LEA/

CMAT, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

Equal Opportunities - Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children.

Parental Involvement

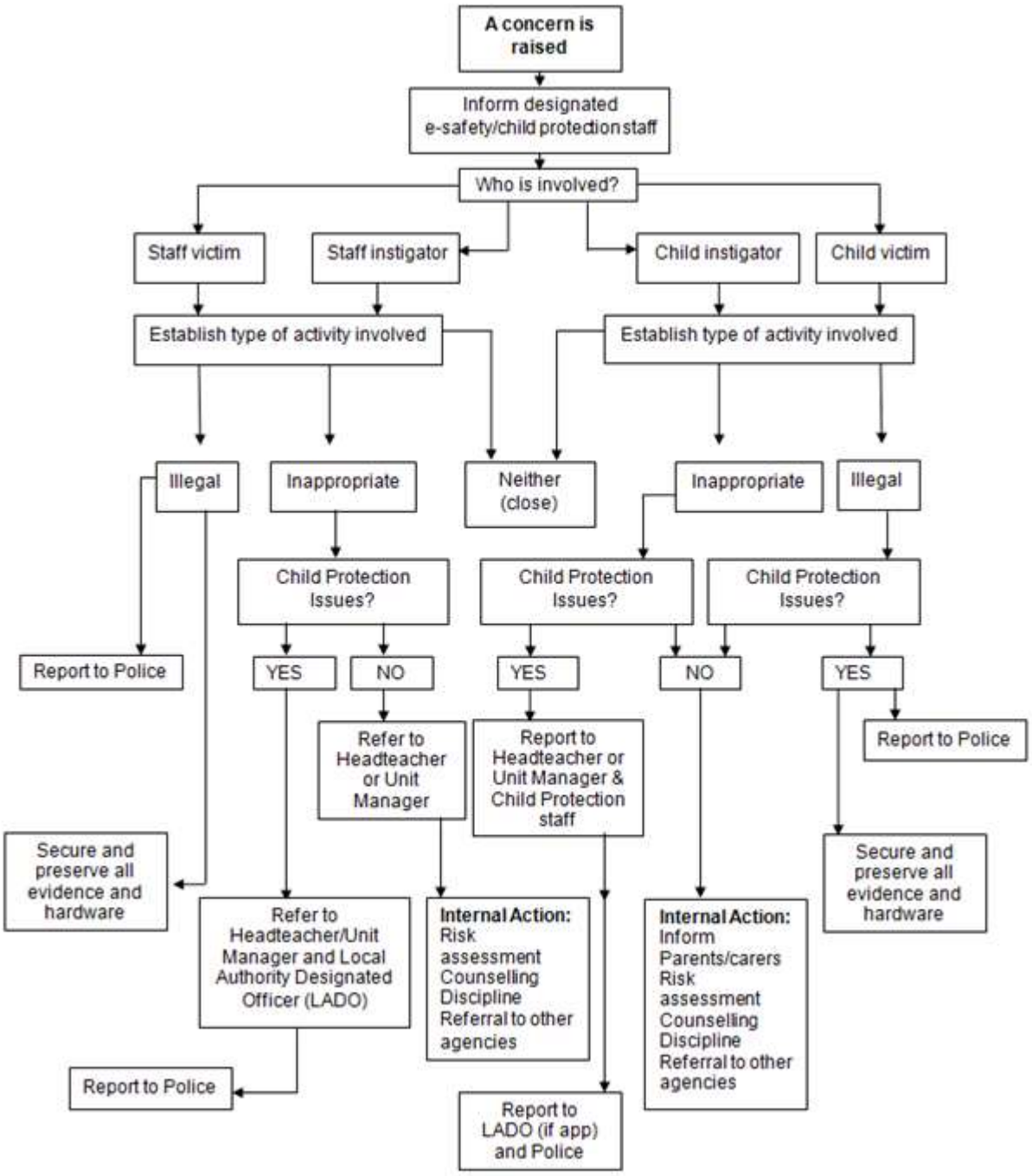
- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school Technology Safety policy by discussion through information events and annual questionnaires.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Guest speakers and workshops
  - Parent pocket guides
  - Posters and handouts
  - Website
  - Newsletter items
  - Tweets

Unsuitable/Inappropriate Activities

School IT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below.



Community use of the Internet

- The school will liaise with local organisations and CMAT to establish a common approach to e-safety if and when it is appropriate.

Introducing the Technology safety policy to pupils

- Phase related E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will know that they have the right to find information using digital sources but only if it is safe.
- There will be an e-safety board in the ICT suite which will be regularly updated.
- Information and guidance of how to access and navigate content, software and hardware effectively and safely will be shared each lesson (in a way that is accessible and relevant to the children and task).

Staff and the Technology Safety policy

All staff will be given the School Technology Safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School Technology Safety Policy in newsletters, the school prospectus, parent pocket guides and on the school website.

Writing and Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the Safety coordinator any issue of E-Safety that concerns them. This policy will be

reviewed bi-annually and consideration given to the implications for future whole school development planning. Staff, Governors, parents and children are given the opportunity to discuss the policy. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix 1: St Norbert's Catholic Primary School

Acceptable Use Agreement / Code of Conduct

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the school E-Safety coordinator.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's Technology Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school

Signature …… Date ……

Job title ……

Full Name ……..(printed)

Signed _____

(Headteacher)

Signed _____

(for and on behalf of the Local Governing Board)

Date _____