Pray, Learn, Achieve and Celebrate Together

E – Safety Policy

A new commandment I give unto you: that you love one another as I have loved you.”

John 13:34

Written: September 2021

Review Date: July 2023

E–Safety Policy Introduction

E-Safety is described as the school's ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

The purpose of this policy is to ensure that all staff, parents, governors and pupils understand and agree the school's approach to E-Safety. The policy relates to other policies including Computing Curriculum, Internet Access, Bullying, Child Protection and Health and Safety. At St Gabriel's we do this by focusing on the 4 C's – Content, Contact, Conduct and Commercialism.

Content: age-inappropriate or unreliable content can be available to children

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need your help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Contact: children can be contacted by bullies or people who groom or seek to abuse them

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. The use of privacy settings online will also allow children to customise the information that each friend is able to access. If a child is the victim of cyberbullying, this can be reported online and offline. Children must understand the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers.

Commercialism: young people can be unaware of hidden costs and advertising in apps, games and websites

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Encourage your children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

E-Safety comes under two strands; Protection and Education. Protection looks at; IT infrastructure, policies, audits, management of personal data and robust reporting mechanisms. Education looks at; staff training, embedding an E-Safety curriculum, support for parents, acceptable use policy and E-Safety agreements.

Protection

Roles and Responsibilities

The Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety Coordinator is Lesley Charlesworth who has been designated this role as a member of the Senior Leadership Team, and works in conjunction with Kelly Lord, Computing Coordinator. There is also a nominated eSafety governor, Father Paul Grady. All members of the school community must be made aware of who holds this post. It is the role of the eSafety Co-ordinator to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and Governors are updated by the eSafety Co-ordinator and all Governors have an understanding of the issues and strategies at the 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, is to protect the interests and safety of the whole community.

IT Infrastructure

Managing filtering

At St Gabriel's we use a managed system where we have control over access to websites. This allows us to access online content dependent on age and appropriate need. The school works in partnership with parents and Abtec the school's Internet Service Provider and Sophos, the school's IT Support to ensure systems to protect pupils are reviewed and improved.

Senior staff and the Computing subject lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective in practice.

The Securus filter system will be checked regularly by senior members of staff and the computing subject lead. If a violation has occurred, it will be dealt with appropriately.

If staff or pupils discover unsuitable websites, images or content. The screen must be switched off/closed and the incident reported. The URL (address) and content must be reported to the Internet Service Provider via the Computing subject lead. This will then be removed and blocked from the school network indefinitely. If a child or a member of staff searches inappropriately or uses a banned phrase, Sercurus will produce a picture of the violation which will send an email to the eSafety Coordinator. This will then be dealt with by senior staff or the Computing subject lead. Parents of children involved will be notified immediately by a senior member of staff if the incident is deemed serious enough or is a repeat offense. Any incidents of this will be recorded on CPOMS by the Computing subject lead.

Equipment

All staff laptops are subject to encryption software and are the only school devices permitted to leave the school site, all other devices must remain in school and are managed in a way that once off site data from the school network cannot be accessed. Removable media must not be used unless they have been proven to be encrypted to a sufficient level and are only used on machines where the Antivirus is up to date. If there are any problems or concerns relating to viruses or antivirus software, the Computing Subject Leader should be informed in person who will then liaise with the school technician. Neither pupils or staff are permitted to download programs or files on school devices without seeking the permission of the Headteacher/Computing Coordinator.

As a school, St Gabriel's is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection

1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998. In the Acceptable Use Policies and contracts Staff and pupils are aware that email and internet activity is monitored, and where required investigated further.

Policies

The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- Acceptable Use Policy for students, staff, governors and visitors
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy

- Staff Code of Conduct
- Home-School Agreement
- Behaviour Policy

These policies are integrated with each other to ensure positive behaviour, safeguarding and anti-bullying. We incorporate an acceptable use policy which is understood and respected by pupils, staff and parents.

These policies procedures and resource materials are available to staff on the staff shared drive and hard copies are available on request.

Authorising internet access

All staff must read and sign the "Staff Code of Conduct" before using any school ICT source.

The school maintains a record of all staff and children who have access to the school's ICT systems.

Parents are asked to sign a consent form regarding their child's internet use (see Acceptable Use Policy).

Any person not directly employed by the school will be asked to read and sign the

"acceptable use of school ICT resources" before being allowed to access the internet from the school site.

Managing the Internet

The internet is pivotal to the running of the school and a vital tool for education. The Schools Acceptable Use Policy defines what is considered acceptable, unacceptable and negligent in terms of the use of the schools internet services. The school provides internet access to all authorised users of the system on approved school equipment only. Each internet accessible machine or device in the school is protected by firewall and web filtering software. In addition to this, monitoring takes place around what is accessed or attempted to be accessed from each machine or device (whether accessed through internet connections within or external to the school) The use of these activities and monitoring logs are checked regularly by staff and reports are sent to designated staff members where any attempts have been made to access inappropriate content. This is immediately followed up with the relevant parties.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and wireless internet technology.

- Staff will, during their lesson planning, check any online content they wish to use with their class.
- Where possible staff must use a safe search engine
- When staff set internet research for homework, they will check and suggest specific sites for use. It is then the parents' responsibility to recheck these and supervise their children's internet use at home.
- 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.

You Tube

The filtering service does not allow children to access You Tube. Staff are permitted to use You Tube clips where no others are available and the following points have been followed:

- Where possible alternative video clips should be sourced
- Clips must be for educational purposes only
- They must be checked thoroughly for any inappropriate content, both at the time of planning and before use
- URLs are included in the lesson plan
- Auto play function must be switched off
- Clips must be loaded and ready to use and passed any adverts prior to the children's viewing.

Social Media (and other 'web 2.0' technology)

The term Web 2.0 technology refers to the way that people now use the internet to share and communicate information and content. This covers but is not inclusive of the following: pod casting, blogging, wikis, content streaming sites and social networking sites. They are fast becoming part of modern life and some aspects of these technologies can be used effectively in the classroom. For example the pod casts and blogs created by children can be used to communicate with parents or each other about learning and school life. Whilst they can be useful and productive, it is important to educate and keep children safe from the dangers of these new technologies.

At Saint Gabriel's we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. This is discussed as part of the Computing Curriculum and during school assemblies, and during eSafety week.

- Through use of the web filtering services, the school endeavours to deny access to social networking sites to pupils within school.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites.
- Pupils are asked to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests). Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

Staff and Social Media

All employees have a personal responsibility for their online behaviour and ensuring their use of social media falls within appropriate professional boundaries. Any inappropriate use of social media by employees which breaches this policy may be treated as misconduct under the schools Disciplinary Procedure for Employees in Schools and could potentially constitute gross misconduct which could result in employment being terminated. If this involves a young person under eighteen years of age, an employee could be referred to the Disclosure and Barring Service and risk being barred from working with children and vulnerable adults.

Employees who choose to use social media should therefore:

- Consider how their online presence could possibly compromise their professional responsibilities. Think carefully before posting information, photographs or comments on the Internet. (Things they might have thought funny at the time could potentially cause embarrassment to them or others and, online records are easy to create, but can be difficult, or in some cases, impossible to remove).

- Exercise caution when divulging personal information online, for example date of birth, home address etc, as this could potentially put them at risk of identity theft.

- Not give out personal contact details to pupils – mobile number, email address etc.

- Consider doing a Google search on their own name to check what information is held online about them. If any content is found that they would prefer not be accessible, they can request that this is removed, by asking the person who uploaded it if the person is known by them, or if appropriate, by using the "report abuse" facility within the particular site.

- Ensure they protect their social media profile by utilising privacy settings so only friends are able to access and comment on their pages.

- Be aware that their information could still appear on friend's pages, which may be publicly accessible.

- Be aware that friends can 'tag' them into photographs which they may not wish to be publicly available – employees should therefore ask people not to tag them into photographs etc without their consent. Employees can also

  'un-tag' themselves from Facebook photographs.

- Maintain an appropriate distinction between professional and personal life. Employees who have an additional relationship with the school, for example if their own children are pupils, or if they are active members of the community should not use online forums to raise any grievances they may have in relation to school.

- Never request/ accept 'personal' Facebook friend requests, or communicate online with pupils, ex-pupils who are under the age of eighteen, or parents if that contact is likely to compromise the employee's professional position or constitute a conflict of interest or call into question their objectivity.

- Check who is "following" them on Twitter and block pupils, ex-pupils and parents from receiving their updates.

- Refrain from identifying their place of work, or making reference to the school on social media sites.

- Ensure that they have a strong password for all social media sites and that electronic security is maintained by password protecting equipment, never sharing passwords and logging out fully after use. This will include ensuring that school and personal property including mobile phones, laptops, I-Pads etc are kept secure, so that children are not able to access them.

- Never make, respond, or take part in an online conversation that includes any offensive, abusive, derogatory, defamatory or inappropriate comments related to colleagues, pupils, parents or the school on any social media sites and be conscious that information they disclose and opinions that are expressed are in the public domain and as such, could potentially bring them and/or the school into disrepute.

- Ensure that their own personal views cannot be misconstrued as them speaking on behalf of school. (an employee is advised to use statements such as, “my view is..” or “in my opinion..”)

- Always comply with schools policies/ guidance on use of technology.

- Never divulge any confidential information relating to school.

- Not use social networking sites for personal use during working hours.

- Not post any photographs or video footage taken at school onto websites without obtaining express written permission to do so.

- In the event that an employee feels they have been a target of cyber bullying or inappropriate online behaviour, keep the evidence (screen prints, emails etc) and report what has happened to the Headteacher, or a member of the Leadership team. However, extreme caution must be exercised in relation to obscene material and staff members should not retain copies of information, but should instead report their concerns immediately to the Headteacher for further investigation.

- Be mindful of their professional responsibilities when using social media and be conscious that managing their online reputation is important for their current and future career. (There is an increasing trend for employers to access social networking sites before interviewing job applicants so there is potential that their online activities could prevent them from progressing in their career). Equally, an employee could face disciplinary action if their employer feels that their use of social networking is inappropriate.

For more on use of social media please see Social Media Policy

Guidelines for Staff on Using Web 2.0 Technologies in the classroom.

- Permission should be gained from the Head teacher.
- Staff should use safe and secure sites.
- Sites used should have log in facilities.
- Sites used must have functions where user and viewer access can be controlled.
- Sites used must have functions for a staff user to approve all content prior to publishing.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using Purple Mash or other systems approved by the Head Teacher.

Mobile technologies

The schools Acceptable use policy outlines the school position on use of mobile technologies with school. However it is important to highlight the following information:

Personal Devices

- Staff members are permitted to bring their mobile phones into school however they must be stored and used only in the designated areas.
- Pupils are not permitted to bring any mobile or digital technologies into school. The school will store any devices brought in by accident at the school office however it does not accept responsibility for the loss, damage or theft for any items brought into school.
- Inappropriate messages sent/posted between or about members of the school community will not be tolerated.
- Visitors to the school are expected to switch their phones off prior to entering the building and permission must be gained from the Head Teacher where images or recordings are required to be taken.
- Anyone bringing these technologies into the building must ensure there is no inappropriate or illegal content on the device.
- Where the school provides technologies for use off site or on visits (laptops, camera equipment and mobile phones) staff are expected to use only the devices given and follow all guidelines set out in the school Acceptable Use Policy

Audit

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school, nor Wigan LA can accept liability for any material accessed, or any consequences of internet access.

The school will regularly;

- Identify new risks
- Influence production or updating of e-safety policies
- Develop good practice
- Identify staff training needs

An audit also takes place at the start of each new year. See appendices.

Safe Use of Images

Taking of Images and Film Digital images are simple to capture, copy and publish and as a result can be misused. 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.

- Where written permission has been sought from parents and staff, the school permits staff and pupils to use school equipment to take appropriate images.
- 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 schools 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.
- On residential trips pupils will be permitted to bring and use disposable camera equipment provided that they use them to take appropriate images and seek consent from staff and children who they wish to take pictures of.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupil's images and work

When a child commences their education at Saint Gabriel's their parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- On the school website
- On the school's Learning Platform
- In the school prospectus or in other printed publications that the school produce for promotional reasons.
- Recorded/ transmitted on a video or webcam
- Put on the display in classrooms and the school's communal areas in display material that may be used in external areas, i.e. 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)

Unless the child's circumstances for consent change (e.g. divorce/custody issues) this agreement will remain in place throughout the child's education at the school. Parents/carers have the right to withdraw this permission, in writing, at any time. The following information will not be published alongside a child's image:

- Pupil's full name
- Pupil addresses
- Pupil emails

Prior to posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Website Coordinator has authority to upload to the site.

Storage of Images

Images/films of children are stored on the school's network and are not permitted to be stored or saved on any portable media (e.g., USB sticks/ SD cards) unless prior permission has been sought from the Head teacher.

Teachers will be allowed right of access to these images within the confines of the school network. Pupils will have limited right of access within the school network, only being able to access images they have stored on their personal user accounts.

The SMT has the responsibility of ensuring the images are deleted when they are no longer required, or the pupil has left the school.

Webcams

We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.

- Misuse of the webcam by any member of the school community will result in
- sanctions (Please see Acceptable Use Policy) Where Webcams are used as part of a learning experience signage must be placed around the area to alert people that filming is taking place.
- Parent permission is gained for this as part of the consent for use of images and recordings.

Managing video conferencing and webcam use

St Gabriel's does not actively promote the use of video conferencing in school however recognises that in some circumstances they may be of benefit to pupils learning experiences. (e.g. a live link up with an international school)

Where staff would like children to take part in a video conferencing experience that links up with those outside of the school community they must ensure the following points are adhered to:

- They must seek permission from the head teacher during the planning phases.
- They must seek written permission from parents and carers. During all processes of the video conference children must be supervised by a member of staff. A record must be kept of all video conferences this should including date, time duration and participants.
- The conferencing equipment must not be set to autoanswer. The conferencing equipment should only be switched on for scheduled and approved conferences.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Managing technologies

- Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day.
- Mobile phones must not be used in school by staff, unless in designated areas or by pupils.

Management and Protection Personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR May 2018.
- Most data is classified as either stage 4 or 5, falling into the restricted or protect category. As a result of this, staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

Email

The use of email is an essential means of communication for staff. In the context of school, email should not be considered private – Freedom of Information and Subject

Access Requests may include email trails, for instance. Educationally, email can offer significant benefits, for instance direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and intended recipient.

Managing Email

The school gives all staff their own email account to use for all school business as a work based tool. This is to minimise 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. The school email account should be the account that is used for all school.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. Staff should never use pupils' personal email addresses under any circumstances.
- All emails should be written and checked carefully before sending, in the same way as a letter written on headed paper.
- Staff must inform the eSafety Coordinator if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work.
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Sending Emails

- Email is an insecure medium. It should not be used for sending personally identifiable or sensitive information (i.e. anything classified as "Protect" or "Restricted" in accordance with the Data Protection policy).
- If you need to send such information within your school, please store the information on the network and simply indicate to the recipient where the information may be found.
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Emails containing sensitive information must be encrypted, this can be achieved when composing an email by clicking on the 3

dots … next to where it states discard and select encrypt. The recipient will receive an email informing them that they have received an encrypted email. It will include instructions on how to open the email.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location on a shared drive / online folder rather than sending attachments.
- School email is not for personal use – and will no longer be available once you leave the school's employment.

Receiving Emails

- Check your email regularly.
- Never open attachments or click on links from an untrusted source. • If in doubt: delete.

Incident Reporting, eSafety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety

Coordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported.

eSafety Incident Log

Any incidents should be reported to and recorded by the eSafety Coordinator in the eSafety log, stored securely in a documented location on the school network (see below)

eSafety Incident Log

Details of Allo safety incidents to be recorded by the safety Coordinator. This incident log will be monitored termly be the Headteacher, member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on a school incident log.

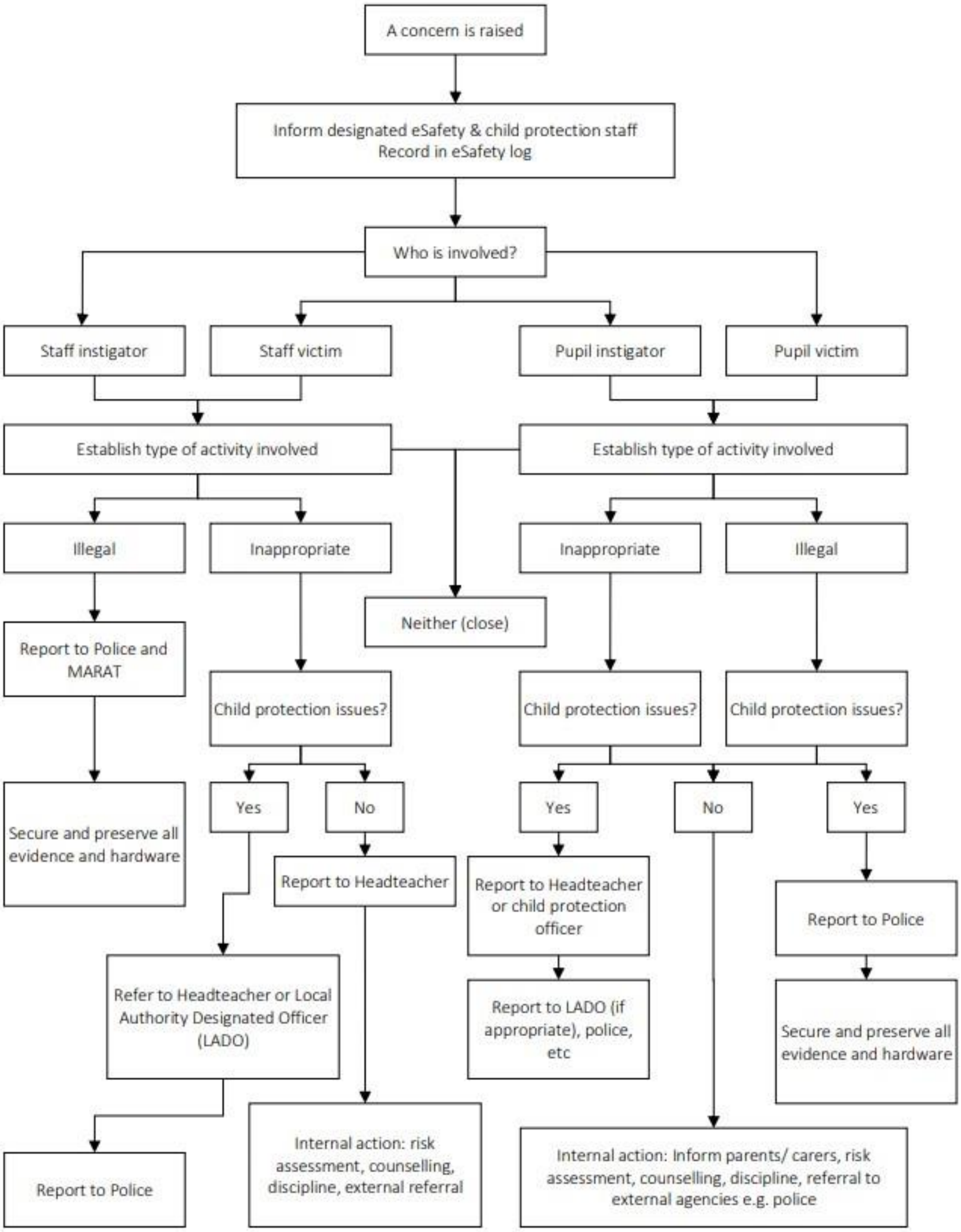
Date & Time	Name of pupil or staff member	Gender	Room & computer or device identifier	Details of incident (including evidence)	Actions & reasons

Handling E-Safety complaints

- Complaints of internet misuse must be referred to the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Policy.
- Pupils and parents are informed of the complaints procedure.
- Pupils and parents are informed of the consequences for pupil misuse of the internet (see below).

Reporting Mechanisms

Flowchart for managing e-Safety incidents


A concern is raised
Inform designated eSafety & child protection staff
Record in eSafety log
Who is involved?
Staff instigator
Staff victim
Pupil instigator
Pupil victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Inappropriate
Illegal
Neither (close)
Report to Police and MARAT
Child protection issues?
Child protection issues?
Child protection issues?
Secure and preserve all evidence and hardware
Yes
No
Yes
No
Yes
Report to Headteacher
Report to Headteacher or child protection officer
Report to Police
Refer to Headteacher or Local Authority Designated Officer (LADO)
Report to LADO (if appropriate), police, etc
Secure and preserve all evidence and hardware
Report to Police
Internal action: risk assessment, counselling, discipline, external referral
Internal action: Inform parents/ carers, risk assessment, counselling, discipline, referral to external agencies e.g. police

Education

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the internet is a necessary tool for staff and students. It helps to prepare students for their on-going career and personal development needs.

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, mobile devices, broadcast media, the internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At St Gabriel's Primary school, we recognise that learning is a lifelong process and that E-Learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate or possibly illegal. E-Safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks. This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

Internet access is provided by Abtec. This includes filtering appropriately to the content and age of pupils. Filtering is provided by Sophos.

Internet access is planned to enrich and extend learning activities.

Access levels are reviewed to reflect the curriculum requirement.

Pupils are given clear objectives for internet use and are expected to sign an Internet Agreement.

Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Pupils are taught how to take responsibility for their own internet access.

E-Safety Curriculum

E-Safety is taken seriously at St Gabriel's. Every class starts the year looking a specific elements of their E-Safety curriculum, this is then looked at again during the week containing Safer Internet day. This will again be followed up by Family Time sessions throughout the year.

Staff and the E-Safety Policy

- All staff are trained regularly and receive a copy of the E-Safety policy.
- Staff are informed that network and internet traffic can be traced to an individual user.
- Staff will always use a child friendly safe search engine where possible when accessing the web with pupils.
- All new staff are 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.

Introducing the E-Safety policy to pupils

- E-Safety rules are posted next to all computers so that all users can see them.
- Pupils are informed that internet use is monitored and appropriately followed up.
- The children are regularly reminded of online safety.
- Pupils are 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 or CEOP report button.
- Students are also aware of websites such as thinkuknow.co.uk

Password security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's safety policy.
- Children from year 1 to 6 are provided with an individual network, and Learning Platform login usernames.
- They are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.

- If children think their password may have been compromised or someone else has become aware of their password it must be reported to Mrs Lord or Miss Charlesworth.

Pupils are taught how to evaluate internet content

- Pupils are taught ways to validate information before accepting that it is necessarily accurate.
- Pupils are taught to acknowledge the source of information, when using internet material for their own use.
- Pupils are made aware that the writer of an email or the author of a webpage might not be the person claimed.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Cyber Bullying

- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyberbullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion.
- Pupils are taught about bullying as part of the PSHE curriculum.
- We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and
- Instances will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying.

Please see Appendices for different forms of cyberbullying.

Sexting

Sexting is defined as 'the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18.' (UKCCIS 2016). It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

It does not include the sharing of sexual photos and videos of under- 18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

The sharing of photos and videos online is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps, such as Snapchat, WhatsApp or Facebook Messenger.

The speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves or others. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Although the production of such imagery will likely take place outside of school, these issues can manifest in schools. We need to be able to respond swiftly and confidently to ensure that children are safeguarded, supported and educated. At St. Gabriel's we have a set procedure to follow.

What to do if an incident involving 'sexting' comes to your attention

Report it to your Designated Safeguarding Lead (DSL) immediately.

- **Never** view, download or share the imagery yourself, or ask a child to share or download – **this is illegal.**
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

For more information please refer to the UK Council for Child Internet Safety document – Sexting in schools and colleges: Responding to incidents and safeguarding young people. A link can be found in the appendices.

Enlisting parents' and carers' support

Parents' and carers' attention is drawn to the school's E-Safety Policy in newsletters, the school brochure and on the school website.

The school has links on its website to E-Safety resources.

The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school; they 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) is allowed. The school disseminates information to parents relating to eSafety where appropriate in the form of:

- Information evenings
- Website postings
- Email
- Twitter • Newsletter items **Appendices**

Staff signatures

I confirm that I have thoroughly read and understood this policy and that I am fully aware of my roles and responsibilities in educating children regarding eSafety issues and maintaining a safe learning environment when using e-technologies and systems.

Name	Role	Signature

Saint Gabriel's Catholic Primary School eSafety Incident log

Details of ALL safety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyber bullying should be recorded on a school incident log.

Date & Time	Name of pupil or staff member	Gender	Room & computer or device identifier	Details of incident (including evidence)	Actions & reasons

Parental/Carer Permission for the use of ICT

I give permission for my child___________________ in Class _____ to take part in/use:

- The Internet
- Web Cameras
- Virtual Learning Networks
- Emailing
- Video Conference sessions

I/We acknowledge that all these activities support an enciting and enriching curriculum and that they will be carried out in line with St Gabriel's Catholic Primary School's e-Safety policy.

I/We support St Gabriel's Catholic Primary School's Acceptable use Agreement and have discussed the e-Safety agreement with my/our child.

Signed ________________(Parent/Carer)

Signed _______________(Pupil)

Date__________________

This Consent form is considered valid for the entire period that your child attends St Gabriel's Catholic School, unless written notification is received.

Forms of cyberbullying

Harassment or trolling

- Sending threats or offensive messages.
- Sharing embarrassing photos and videos.
- Posting upsetting or threatening messages on social networks.

Denigration

Spreading fake or untrue information to spread rumours. The information might be posted on a web page or shared by others using e-mail or instant messaging.

Flaming

Using extreme language to cause a fight. Usually this occurs in a 'public' setting such as a chat room, online forum or comment section rather than private messaging. When a series of insults are exchanged, a 'flame has been lit'. Although it might seem that both people are equal, the perpetrator might say something particularly insulting or nasty to gain the upper hand.

Griefers in online games

A griefer is someone who is less concerned with winning a game and more focused on ruining the game for other people. They will target people with epilepsy for example, by programming strobe lighting into a game to trigger epileptic seizures.

Impersonation

Stealing someone's identity or hacking into someone's site, enabling the perpetrator to pose as the victim. The perpetrator might use the victim's account to post explicit messages that are then shared with their friends and family, to humiliate the victim.

Exclusion

Intentionally leaving someone out.

Sexual cyber bullying (Sexting)

Sending naked or sexual images to a partner who then shares is across social media to embarrass and humiliate the person.

Cyberstalking

Repetitively harassing and sending threatening communications to another person.

Resources and help

www.thinkuknow.co.uk – CEOP's one-stop shop for internet safety. Has a section for teachers and trainers to access free resources

www.digital-literacy.org.uk – SWGfL have created this collection of digital literacy resources for all age groups

www.childnet.com – Video's and resources available for children, young people, parents and professionals. Includes resources designed for younger children such as Smartie the Penguin and Digi Duck

www.saferinternet.org.uk – Collects resources, links, research and guidance for all ages, professionals and parents included

www.wiganlscb.org.uk – Wigan Safeguarding Children Board website with information on internet safety for parents, professionals, children and young people

http://twitter.com/wiganlacb - The LSCB run a Twitter page regarding technology and internet safety. Follow us @wiganlscb

https://www.gov.uk/government/publications/sexting-in-schools-and-colleges - Guidance for schools and colleges on responding in instances of 'sexting'.

Support

www.childline.org.uk – Offers an online and phone based counselling and support service. Will not appear on phone bills and is a Freephone number – 0800 1111 www.kooth.com – An anonymous online counselling service for young people in Wigan

www.iwf.org.uk – The Internet Watch Foundation is an internet industry funded body who seek to remove images of child abuse from the internet

www.cybermentors.org.uk – An online anonymous forum where children and young people can discuss their experiences of being bullied with their peers

CEOP also offer an online 'Report Abuse' button which can be accessed at www.thinkuknow.co.uk

E-Safety Audit

Question	Details
Does the education setting have an eSafety Policy in place that complies with CYPD guidance?	
Date of last update How can staff access the policy?	
Who is the Designated Safeguarding Lead (DSL)?	
How do parents access the e-Safety policy?	
Has e-Safety training been provided to both students and staff?	
Have all staff signed an ICT Code of Conduct on appointment?	
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	
Are e-Safety Rules placed on laptops?	

Is Internet access provided by an approved educational internet service provider that complies with DfE requirements for safe and secure access?	
Has the school's filtering policy been approved by the Senior Management Team?	
Do all staff understand e-safety issues and risks?	
Do students know how to report any concerns they may have when using the internet?	
Are all e-Safety incidents logged?	
Can staff request to block a website to the Computing Coordinator?	

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

- http://www.hmso.gov.uk/acts/acts 1998/19980029.htm

The Telecommunications (Lawful Business Practice) • (Interception of Communications) Regulations 2000

- http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. • http://www.hmso.gov.uk/acts/acts 2000/20000023.htm

Human Rights Act 1998

- http://www.hmso.gov.uk/acts/acts 1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006 It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003 The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information www.teachernet.gov.uk

Communications Act 2003 (section 127) Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 - 3) Regardless of an individual's motivation, the Act makes it a criminal offence to gain: - access to computer files or software without permission (for example using another persons password to access files) - unauthorised access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or program UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1) This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988 Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29) This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. **Protection of Children Act 1978 (Section 1)** It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964 Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997 A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Digital Economy Act 2017 This law deals with communication online. It provides information about what should happen when someone breaks the law. The Act requires social media platforms across the UK to follow a code of Practice which sets out the actions that must take to protect individuals from bullying, intimidation and insulting behaviour online.