Online Safety Policy

(based on LGfL guidance)

St. Vincent's Catholic Primary School

Together through Christ we grow and learn

Date of Policy: September 2019   **Date of Review:** September 2020
Person Responsible: Marina Coleman, Danielle Duffy & Holly Carruthers
Presented to Staff and Governors: September 2019

1.   **Aims**
The purpose of this policy is to:
- set out the key principles expected of all members of the school community at St. Vincent's Catholic Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St. Vincent's Catholic Primary School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content
- exposure to illegal, inappropriate or harmful content, including online pornography, fake news, racist or radical and extremist views (KCSIE 2019), ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact
- being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults (KCSIE 2019)
- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct
- personal online behaviour that increases the likelihood of, or causes harm; for example making, sending and receiving explicit images or online bullying (KCSIE 2019)
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- (Ref Ofsted 2013)

Scope
This policy applies to all members of St. Vincent's Catholic Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St. Vincent's Catholic Primary School.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic

devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

2.   Implementation

Pupil online safety curriculum
This school:
- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on 3BM online safely framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - [for older pupils] to understand that not everything they find on the internet is the truth, and to be aware of false websites and information;
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;
  - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign annually.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Expected conduct

In this school, all users:
- o are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- o need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- o need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- o should understand the importance of adopting good Online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- o will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff
- o are responsible for reading the school's Online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils
- o should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers
- o should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the school
- o should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management
In this school:
- o there is strict monitoring and application of the Online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- o all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- o support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online safety issues
- o monitoring and reporting of Online safety incidents takes place and contribute to developments in policy and practice in Online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- o parents / carers are specifically informed of Online safety incidents involving young people for whom they are responsible.
- o We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Internet access, security (virus protection) and filtering
This school:
- o Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- o Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- o Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

- o Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- o Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- o Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- o Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- o Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- o Uses security time-outs on Internet access where practicable / useful;
- o Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- o Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- o Ensures all staff, students and parents have signed an acceptable use agreement form each year and understands that they must report any concerns;
- o Ensures pupils only publish within an appropriately secure environment: the school's learning environment or LGfL secure platforms such as J2Bloggy, etc.
- o Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. primaryICT or KidRex , Google Safe Search , …..
- o Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- o Informs all users that Internet use is monitored;
- o Informs staff and students that that they must report any failure of the filtering systems directly to the Headteacher and log on the ICT problems folder. Our system administrator(s) 3BM logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- o Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- o Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- o Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)
This school
- o Uses individual, audited log-ins for all users - the London USO system;
- o Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- o *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- o Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- o Storage of all data within the school will conform to the UK data protection requirements
- o Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:
- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different / use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 1 they are also expected to use a personal password;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;

- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Has an automatic lock system on all staff computers if they have been inactive for 15mins (5mins for Head and Deputy). Teachers are requested to manually lock their computers if they are leaving them unattended.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager ; equipment installed and checked by approved Suppliers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access register;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems: *e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. 3BM technical support
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy
- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This school
- Provides staff with an email account for their professional use, *London Staffmail* and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@stvincentsprimary.org.uk, for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:
- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection..
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:
- Staff can only use the LA or LGfL e-mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX,

Online Safety Policy   St Vincent's Catholic Primary School   September 2019

- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website
- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers:
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@stvincentsprimary.org.uk Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy. E.g.

School staff will ensure that in private use:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing
This school
- Only uses the LGfL / Janet supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV
- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.
- Please refer to CCTV Policy

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

Online Safety Policy   St Vincent's Catholic Primary School   September 2019

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record maintained by the Senior Administration officer.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed. This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions
- Staff have their own designated area on the network to store sensitive documents.
- We require staff to log-out of systems when leaving their computer.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use VPN solution with its 2-factor authentication for remote access into our systems.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use Redstor for disaster recovery on our network
- We comply with the WEEE directive on equipment disposalby using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data (arranged through 3BM).
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

Equipment and Digital Content

Personal mobile phones and mobile devices
- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones are only allowed on the final term of Year 6 with permission form the Headteacher. Mobile phones which are brought into school are handed in and must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a senior member of staff.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices
- The School only allows student mobile phones should to be brought into school in the final term of Year 6 as part of the secondary transition support program.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Staff use of personal devices
- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

3.   Key Responsibilities

Governing Body
- Ensure that the school follows all current e-safety advice to keep the children and staff safe
- Approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. Support the school in encouraging parents and the wider community to become engaged in e-safety activities
- A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:
  - regular review with the Online Safety Co-ordinator / Officer (including online safety incident logs, filtering / change control logs)

Headteacher/ Online safety Lead
- Takes overall responsibility for Online safety provision and a leading role in establishing and reviewing the school e-safety policies / documents
- Takes overall responsibility for data and data security (SIRO)
- Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL
- Is responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant
- Is aware of procedures to be followed in the event of a serious online safety incident.
- Ensures that there is a system in place to monitor and support staff who carry out internal Online safety procedures(e.g. network manager)
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Ensures that Online safety education is embedded across the curriculum
- Liaises with school ICT technical staff
- Communicates regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident
- Ensures that an Online safety incident log is kept up to date
- Facilitates training and advice for all staff
- Liaises with the Local Authority and relevant agencies
- Is regularly updated in Online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - cyber-bullying and use of social media

LGfL Nominated contact(s)
- Ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts

Classteachers
- Embed Online safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Staff
- Read, understand and help promote the school's Online safety policies and guidance
- Read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
- Are aware of safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- Report any suspected misuse or problem to the Online safety coordinator
- Maintain an awareness of current Online safety issues and guidance e.g. through CPD
- Model safe, responsible and professional behaviours in their own use of technology
- Ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Jartech / Technical Support
- Report any e-safety related issues that arises, to the online-safety coordinator.
- Ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- Ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)
- Ensure the security of the school ICT system
- Ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- Ensure the school's policy on web filtering is applied and updated on a regular basis and that LGfL is informed of issues relating to the filtering applied by the Grid
- Keeps up to date with the school's online-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
  - Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Pupils
- Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- to understand the importance of reporting abuse, misuse or access to inappropriate materials
- to know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
  to help the school in the creation/ review of Online safety policies

4.   Monitoring and Reporting
The policy will be communicated to staff/pupils/community in the following ways:
- Policy to be posted on the school network
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:
The school will take all reasonable precautions to ensure Online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview with Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period
  - referral to LA / Police.
- Our Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The Online safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies .
- The school has an Online safety coordinator who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the school Online safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online safeguarding policy will be discussed in detail with all members of teaching staff.

Staff and governor training

This school
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program
- Provides as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school
- Runs a rolling programme of advice, guidance and training for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safety behaviour are made clear
- Information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

5.   Opportunities for Spiritual and Moral Development

In Catholic education, we are aware that all knowledge and understanding comes from God. In Online Safety we will provide opportunities for pupils' spiritual and moral development by encouraging all pupils to stop and reflect at the wonder of technology, the speed of communication and the power of the microchip.

6.   Equal opportunities

We should ensure that the specified aims are implemented for all children regardless of race, religion, gender, ability and disability. We will do this by:
- o Ensuring all children should have access to the use of ICT regardless of gender, race, cultural background or physical or sensory disability. Where use of a school computer proves difficult for a child because of a disability, the school will endeavour to provide specialist equipment and software to enable access. Children with learning difficulties can also be given greater access to the whole curriculum through the use of ICT. Their motivation can be heightened and they are able to improve the accuracy and presentation of their work. This in turn can raise self-esteem.
- o Planning for ICT in the early years needs to be considered carefully if children are to begin to gain confidence in the use of ICT as soon as they start attending Nursery. A range of appropriate hardware, software and activities needs to be offered
- o Planning needs to match the learning opportunities offered with the children's age, abilities and skills. Task matching may include provision of different software, varying the amount/type of support given, varying the tasks, varying the groupings etc.

7.   Health and Safety
- Online Safety should be addressed regularly in Computing lessons, PSHCE lessons, assemblies and through the use of Hector the Protector.
- Children should not be responsible for moving heavy equipment around the school. They may not load software and should not be given the responsibility of plugging in and switching machines on without a member of staff present.
- Food and drink should not be consumed near ICT equipment.
- It is the responsibility of staff to ensure that classroom ICT equipment is stored securely, cleaned regularly and that their class or themselves leave the ICT Suite clean and tidy after use.
- Staff should ensure that the children are seated at the computers comfortably and be aware of the dangers of continuous use (e.g. eye/wrist strain etc).
- Children must not look at the laser of IWB and be warned of the dangers in doing so.
- An adult should always supervise children when they are accessing information via the Internet. All children, parents and staff must sign an Acceptable Use Agreement (in line with the AU Policy). The service provider does filter information but staff are ultimately responsible for information accessed by pupils.

Useful Links:

Protocol for responding to online safety incidents
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Keeping Children Safe in Education September 2019

Appendix A

Keeping Children Safe in Education September 2019
Annex C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and monitoring
Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.UK Safer Internet Centre: appropriate filtering and monitoring. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like:

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G,4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Reviewing online safety.

Online Safety Policy   St Vincent's Catholic Primary School   September 2019

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCCIS have recently published Online safety in schools and colleges: Questions for the governing board

Staff training
Governors and proprietors should ensure that as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support
There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk
www.parentzone.org.uk
www.childnet.co.uk
www.net-aware.org.uk
www.commonsensemedia.org.uk
www.educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/
https://www.gov.uk/government/publications/searching-screening-and-confiscation
https://www.lgfl.net/online-safety/default.aspx