St Vincent's Catholic Primary School

Policy for Acceptable Use of the Internet and Related Technologies

Contents

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

It is our duty to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the children, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The head teacher is the e-safety coordinator and keeps up to date with e-safety issues and guidance. She keeps the governors updated with all e-safety issues.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff are familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.

Complaints regarding e-safety

The school will take all reasonable precautions to ensure e-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/class-teacher Year / e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint.

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

Managing Internet Safety

At St Vincent's

- We supervise pupils' use at all times, as far as is reasonable.
- We use the LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments.
- Teachers plan the curriculum context for Internet use to match pupils' ability, using Google search engine – Google images is restricted by filter.
- We inform staff and pupils that that they must report any failure of the filtering systems directly to the teacher, deputy head, Headteacher. Our systems administrators report to LA / LGfL where necessary;
- All Chat rooms and social networking sites are blocked by our LA filtering system.
- We require pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme.
- We require all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- All users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

We keep a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;

- We ensure the named child protection officer has appropriate training;
- We ensure parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the school;
- We make information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- We immediately refer any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Staff at St Vincent's

- Foster a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Headteacher;
- Ensure pupils and staff know what to do if there is a cyber-bullying incident;
- Ensure all pupils know how to report abuse;
- Have a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
  - to STOP and THINK before they CLICK
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - 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 some search engines / web sites that are more likely to bring effective results;
  - to know how to narrow down or refine a search;
  - to understand 'Netiquette' 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 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, 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;

- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensure staff understand data protection and general ICT security issues linked to their role and responsibilities;
- Make training available annually to staff on the e-safety education program;

Managing e-mail

At St Vincent's we use a filtered Internet-based e-mail system through the London Grid for Learning (LGfL).
We don't have individual pupil email accounts. Older pupils email work to school, which is then accessed by the relevant teachers and saved onto the server.

- We do not publish personal e-mail addresses of pupils or staff on the school website. We use general.post@st-vincents.bromley.sch.uk for any communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
- Accounts are managed effectively, with up to date account details of users
- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make e-mail dangerous. LGFL filters most unsuitable emails.

Pupils:

- Staff can only use the LGfL / school domain e-mail accounts on the school system.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- We use whole-class or group e-mail addresses at Key Stage 2 and year 2 below, eg year3@st-vincents.bromley.sch.uk.
- Pupils are taught about the safety and 'netiquette' of using e-mail i.e.
    - not to give out their e-mail address unless it is part of a school managed project or 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;
  - the sending of attachments should be limited;
  - 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;

- Pupils sign the school Agreement Form 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.

Staff:

- Staff use LGfL e-mail systems for professional purposes;
- Access in school to external personal e-mail accounts is blocked;
- e-mail sent to an external organisation is written carefully, and requires authorisation, in the same way as a letter written on school headed paper.
  - the sending of attachments should be limited;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

- Staff sign the school Agreement Form 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.

<u>Social networking and personal publishing</u>

- Access to social networking sites is blocked.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a

photograph which could identify the student or his/her location eg. house number, street name or school.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Use of Digital and video images

At St Vincent's we do not use photographs or video footage of pupils on the school website.

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the Headteacher the Deputy Headteacher and the administration officer The school web site complies with the school's 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 and telephone number. Home information or individual e-mail identities are not published;
- 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;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network.
- 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;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;

Managing Equipment

To ensure the network is used safely at St Vincent's we

- Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access. They are given class access to the school curriculum network.
- Make it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Have 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;
- Require all users to 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.
- Make 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 (Sophus);
- Make 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.
- Make clear that staff accessing LA systems do so in accordance with Bromley's policies;
  e.g. Borough email and Intranet; finance system, Personnel system etc
- Maintain equipment to ensure Health and Safety is followed;
- Have separate curriculum and administration networks, access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Do not allow any outside Agencies to access our network remotely;
- Use the DfES secure s2s website for all CTF files sent to other schools;
- Ensure 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;
- Have firewalls and routers that have been configured by the LA to prevent unauthorised use of our network;
- Review the school ICT systems regularly with regard to security.

Infringements of the AUP

Any infringement of the signed agreement will be dealt with appropriately.

What to do if

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the headteacher and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the headteacher and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.

Consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

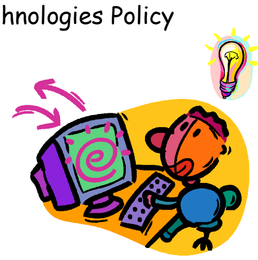
Cyberbullying

Bullying can be done verbally, in writing or images, **including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites.** It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender's e-mail service provider
5. Notify parents of the children involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the LA e-safety officer

E-safety agreement form: staff



Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email, with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the head or deputy head teacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will

notify the school of any “significant personal use” as defined by HM Revenue & Customs.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school’s e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any Bromley policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school’s ICT resources and systems.

Signature ....Date ....

Full Name .... (printed)

Job title ....

School St Vincent’s Catholic Primary School

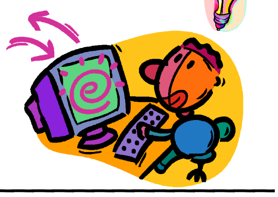
Authorised Signature

I approve this user to be set-up.

Signature .... Date...

Full Name Deirdre Wright

E-safety agreement form: parents



Parent / guardian name: ____________________________________

Pupil name(s): ____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL e-mail* and other ICT facilities at school. I have been informed that children are supervised whilst using the Internet. (children in the Reception Class do not use the Internet)

I know that my daughter or son will be asked to sign an e-safety agreement form when they reach Year 3 and that they will be given a copy of the 11 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: ________________________________

Date: ___/___/___

- -

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images', which is attached. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: ___________________________ Date: ___/___/___

* At this school we only use the London Grid for Learning email system with pupils. We do not set-up individual email accounts. Where we choose to let pupils communicate with others outside of the school, we only do so with those approved by the school. We tell pupils to never give out their private email addresses to strangers unless they have approval.

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

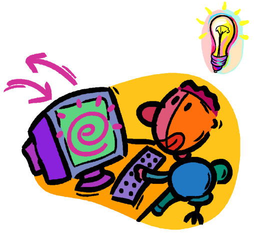
Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.
- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's photograph could appear in the media if a newspaper photographer or television film crew attend an event, in this case you will be specifically asked for written permission;

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Further information for parents on e-Safety can be found at:
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Keeping safe: stop, think, before you click!



11 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will not look at other people's files without their permission.
- I will only delete my own files.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission. This means by email or on websites, texts, instant messaging, social networks eg face book twitter or in any other way.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult. I know I will not get into trouble for having accessed something I shouldn't have if I report it.
- I will report any cyber bullying, whether it happens at home or at school. I will either tell someone in my family or someone at school.

These rules were made and agreed by the children at St Vincent's Catholic Primary School to keep us safe