St Vincent's Catholic Primary School

Online Safety Policy

November 2017

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

This policy should be read in conjunction with appendix 8: Infringements

Contents

Appendices

Appendix 1: Acceptable Use Agreement (Staff, Volunteers and Governors)

Appendix 2: Acceptable Use Agreements (Pupils – adapted for key stage)

Appendix 3: Acceptable Use Agreement including photo/video permission (Parents)*

Appendix 4: Sexting: how to respond to an incident UKCCIS

Appendix 5:
http://www.ticbradford.com/downloads/esafeguarding/teachers/216-first-line-information-support-for-esafety-incidents/file - page 23 onwards

Appendix 6: Prevent: Radicalisation and Extremism

Appendix 7:

Data security: Use of IT systems and Data transfer

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

Appendix 8: Infringements

Appendix 9: 'What to do if?: guide for staff

1. Introduction and Overview

Rationale

At St Vincent's Primary School we fully understand the need for pupils to access and be taught skills in ICT in order to prepare them for working with ICT technologies in the future. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the school is bound. At St Vincent's through this Online Safety Policy, we ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

As with all other risks, it is impossible to eliminate those risks completely, it is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The Department for Education's (DfE) 2016 Keeping Children Safe in Education (KCSIE) statutory guidance states that "Governing bodies and proprietors should ensure there are appropriate procedures in place...to safeguard and promote children's welfare ...which should amongst other things include... acceptable use of technologies...and communications including the use of social media."

The purpose of this policy is to:

Set out the key principles expected of all members of the school community at St Vincent's with respect to the use of IT-based technologies.

Safeguard and protect the children and staff.

Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.

Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies – behaviour and anti-bullying policy].

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 pupils.

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

Content

Exposure to inappropriate content

Lifestyle websites promoting harmful behaviours

Hate content

Content validation: how to check authenticity and accuracy of online content

Contact

Grooming (sexual exploitation, radicalisation etc.)

Online bullying in all forms

Social or commercial identity theft, including passwords

Conduct

Aggressive behaviours (bullying)

Privacy issues, including disclosure of personal information

Digital footprint and online reputation

Health and well-being (amount of time spent online, gambling, body image)

Sexting

Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of St Vincent's Primary School community (including staff, pupils/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of St Vincent's IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 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 e-safety behaviour that take place out of school.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. To take overall responsibility for online safety provision To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. CBC services To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles To be aware of procedures to be followed in the event of a serious online safety incident Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised To receive regular monitoring reports from the Designated Safeguarding Lead To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. IT technician To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety To ensure school website includes relevant information.
Designated Safeguarding Lead	Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents Promote an awareness and commitment to online safety throughout the school community Ensure that online safety education is embedded within the curriculum Liaise with school technical staff where appropriate To communicate regularly with SLT and the designated online safety Governor (Safeguarding Governor) to discuss current issues, review

Role	Key Responsibilities
	incident logs and filtering/change control logs To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident To ensure that online safety incidents are logged as a safeguarding incident Facilitate training and advice for all staff Oversee any pupil surveys / pupil feedback on online safety issues Liaise 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 concerns.
Governors/Safeguarding governor (including online safety)	To ensure that the school has in place policies and practices to keep the children and staff safe online To approve the Online Safety Policy and review the effectiveness of the policy To support the school in encouraging parents and the wider community to become engaged in online safety activities The role of the online safety Governor will include: regular review with the DSL
Computing Curriculum Leader	To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician	To report online safety related issues that come to their attention, to the DSL To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the

Role	Key Responsibilities
	DSL/Headteacher To ensure appropriate backup procedures and disaster recovery plans are in place To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Business Manager/ Office staff/ SENDco/ DSL)	To ensure that the data they manage is accurate and up-to-date Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. The school must be registered with Information Commissioner
Nominated contact(s) (Headteacher/ Business Mananger/ IT Technician)	To ensure all CBC services are managed on behalf of the school following data handling procedures as relevant.
Teachers	To embed online safety in the curriculum To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP (Appendix 1) is signed by new staff on induction. To report any suspected misuse or problem to the DSL To maintain an awareness of current online safety issues and guidance e.g. through CPD To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually. (AUP Appendix 2) 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 understand the importance of adopting safe behaviours and 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 To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren. (AUP – Appendix 3) to consult with the school if they have any concerns about their children's use of technology to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school to support the school in promoting online safety To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff have guidelines 'What to do if' to follow. Appendix 9
- Staff and pupils are given information about infringements in use and possible sanctions.
- DSL acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to DSL that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" (Appendix 4) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services

- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult

2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)

3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

4. The imagery involves sexual acts and any pupil in the imagery is under 13

5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- 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 safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- 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 Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- runs a rolling programme of online safety advice, guidance and training for parents, through leaflets and workshops.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school 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;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;

- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

In this school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the CBC services;
- uses the CBC filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses CBC user-level filtering where relevant e.g. you tube;
- ensures network health through use of Sophos anti-virus software (from CBC services);
- Uses DfE or LA approved systems including DfE S2S, Sophos, Any Comms secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the CBC Services to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

Network management (user access, backup)

In this school:

- Uses individual, audited log-ins for all users - the CBC system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/network manager is up-to-date with CBC Services and policies/requires the Technical Support Provider to be up-to-date with CBC Services and policies;
- Has daily back-up of school data for admin and curriculum. (currently in process of setting up);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance (currently in process of setting up);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU. Current data is stored using the RMG2 Integris system

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.
- All pupils in year 5 and 6 have their own unique username and password which gives them access to the schools email;
- 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;
- 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 log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data (currently in process of setting up);
- This school uses secure data transfer; this includes 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 Local Authority (AnyComms).
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

In this school:

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.

E-mail

In this school:

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- 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
- We use a number of CBC-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

In this school:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

In this school:

- Staff can only use the schools e mail systems on the school system
- Staff will use the schools e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

In this school:

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- 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;
- 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;

Cloud Environments

In this school:

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

In this school:

- Staff are instructed to always keep professional and private communication separate.
- 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 pupils, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- 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 academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

In this school:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

In this school:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Video recording:

In this school:

- 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.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

In this school:

- The Business Manager 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 a single central record

Technical Solutions

In this school:

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the CBC AutoUpdate, for creation of online user accounts for access to broadband services and the CBC content.
- All servers are in lockable locations and managed by DBS-checked staff.
- 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.
- 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.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

In this school:

- Mobile devices brought into school are entirely at the staff member, pupils & 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.
- Mobile devices are not permitted to be used in areas where pupils are present. 'Mobile-free' signs to this effect are displayed.
- Personal mobile devices will not be used during lessons.
- No images or videos should be taken on mobile devices without the prior consent of SLT.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

Storage, Synching and Access

The device is accessed with a school owned account

In this school:

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.
- The device is accessed with a personal account
- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Pupils' use of personal devices

In this school:

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- Pupils need parental and school permission to bring his or her mobile phone into school. Any other mobile device brought into school will be confiscated.
- All pupil mobile devices will be handed in at reception should they be brought into school. They 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.
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

In this school:

- No staff personal devices (except mobile phones) are permitted to be used on the school site.
- Mobile Phones will be switched off or switched to 'silent' mode.
- Mobile phones will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities.
- 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 and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

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, high profile use
- The school blocks/filter access to social networking sites 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 computing 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 identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Name of School	**St Vincent's Catholic Primary School**
Policy review Date	**November 2017**
Date of next Review	**November 2018**
Who will review this policy?	**SLT and Computing Lead**

Appendix 1:

Jesus, be the centre of our lives

E-Safety Acceptable User Policy

Staff COPY

Teaching and Support Staff

Member of Staff: .....

School Policy

The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness to support learning. All users have an entitlement to safe internet access at all times.

The school will try to ensure that staff will have good access to ICT to enhance their teaching and pupils' learning and will, in return, expect the staff to agree to be responsible users.

This Acceptable Use Policy is intended to ensure:

- All staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

This policy must be read in conjunction with the school's Online safety policy. By signing this policy you are stating that you have also read the Online safety policy and agree to abide by all the terms and guidelines within both policies.

If a member of staff is not willing to sign this policy, so indicating that they do not accept the terms within this and the Online safety policy, then he/she will not be able to use any of the school's ICT devices nor access any of the school's on-line facilities.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the pupils in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. A central record of individual passwords will be kept by the ICT Network Manager.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I understand that usage of school ICT systems outside of school by family members needs to primarily focus on educational use and that use of the systems for personal or recreational use will be in line with the policies and rules set down by the school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- If I choose to use my personal equipment to record images during the school day or on schools trips I will download them to school equipment by the end of the next school day. I will remove all images from the equipment once downloaded. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites outside of school for personal use and will never communicate anything relating to school community – see Online safety policy.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities – refer to the **Online safety policy** for further guidance.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use (refer to the **Online safety policy** for further guidance). I will ensure all personal devices are password protected.
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will ensure that my data on school laptops and external storage devices is regularly backed up,
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software, apps or online tools that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads outside or within teaching hours to avoid taking up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. Before downloading any software, either for school or personal use, the appropriate form must be completed and returned to the e-safety co-ordinator to be authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission or use appropriate acknowledgement to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations (including outside of school) related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and the removal of equipment access. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the terms and guidelines set out in the Acceptable User Policy for staff and in the school's Online safety policy. I agree to use the school's ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) as detailed in these terms and guidelines. I also agree to the terms and guidelines relating to the use of services and sites accessed through the internet (both on the school's or my own personal ICT equipment) in order to communicate with, or in relation to, members of the school community.

Name: .....

Signature: .....

Date:

.....PLEASE SIGN

AND RETAIN THIS POLICY.

Appendix 2

E-Safety Acceptable User Policy

PUPIL COPY

Early Years & KS1Pupils

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETAINED BY PARENTS.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices without permission:

- ☹ Mobile phones, including Smart Phones, Blackberries, iPhones
- ☹ Mobile Devices including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Cameras including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony PlayStations, The MG Portable Android Gaming System

I agree that I will:

- always keep my passwords a secret;
- talk to my teacher before using anything new on the internet;
- ask permission before signing up to any websites and always use my learning platform email address to do so;
- tell my teacher if anything makes me feel scared or uncomfortable;
- make sure all messages/postings I send or write are polite;
- show my teacher if I get a nasty message;
- not reply to any nasty message or anything which makes me feel uncomfortable; not
- give my mobile phone number to anyone who is not a friend in real life; only email or
- message people I know;
- when I am at school, I will only use my school email address;
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets);
- not load photographs of myself and others onto the computer, unless with the permission of my teacher;
- never agree to meet a stranger.

Anything I do on the computer may be seen by someone else

Pupil signature:_____ Date: _____

Parents/Carers

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and when using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I have read this E-Safety Acceptable User Policy and have discussed it with my child. I

agree/do not agree (delete as appropriate) to support the school's policy on e-safety.

Please be aware that if you do not sign the agreement to support the school's policy on e-safety, your child will be unable to use ICT equipment, or to have access to the internet, in school.

Signed: (Parent/Guardian/Carer): _____

Date: _____

E-Safety Acceptable User Policy

Pupil COPY

KS2 Pupils

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETAINED BY PARENTS.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices without permission:

- ☹ Mobile phones, including Smart Phones, Blackberries, iPhones
- ☹ Mobile Devices including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Cameras including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony PlayStations, The MG Portable Android Gaming System

*I will only bring in a mobile phone if I walk home alone and have permission from my parents and the school. I will leave my phone in the School Office during the day.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Ask permission before signing up to any websites and always use my learning platform email address to do so;
- I will act responsibly when sharing or publishing work online and not breach copyright.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for non – educational on-line gaming, internet shopping, file sharing, or inappropriate video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain security to ensure the smooth running of the school:

- I will only use my personal devices (e.g. memory sticks) in school, if I have permission, as these may carry viruses.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission or use appropriate acknowledgement to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour towards any member of the school community when I am out of school (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, the school will take action in line with the Promoting Good Behaviour Policy. This may also include loss of access to the school network / internet, learning platform email and messaging tool, contact with parents/carers and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to be a responsible user and stay safe while using the internet and other communications technologies, both in and out of school, for learning, personal and recreational use.

Pupil signature: _____

Date: _____

Parents/Carers

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and when using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I have read this E-Safety Acceptable User Policy and have discussed it with my

child.

I agree/do not agree (delete as appropriate) to support the school's policy on e-

safety.

Please be aware that if you do not sign the agreement to support the school's policy on e-safety, your child will be unable to use ICT equipment, or to have access to the internet, in school.

Signed: (Parent/Guardian/Carer): _____

Date: _____

Appendix 3 – Photography guidance for parents/ visitors*

*To be inserted

Appendix 4

Sexting: how to respond to an incident

An overview for all teaching and non-teaching staff in schools and colleges

UK COUNCIL FOR **CHILD INTERNET SAFETY**

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.

All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.

The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), ***Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People***, and should **not** refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), 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**. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

'Sexting' 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.

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.

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies should outline codes of practice to be followed.

For further information

Download the full guidance Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016) at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

Appendices 5, 6 and 7 and large documents and accessible by using the online links below.

Appendix 5:
http://www.ticbradford.com/downloads/esafeguarding/teachers/216-first-line-information-support-for-esafety-incidents/file - page 23 onwards

Appendix 6: Prevent: Radicalisation and Extremism:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Appendix 7:

Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/554415/searching_screening_confiscation_advice_Sept_2016.pdf

Appendix 8: How will infringements be handled?

Whenever a pupil or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher and will reflect the school's behaviour and disciplinary procedures.

PUPIL	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email and communications tools • Unauthorised use of mobile phone/personal device in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher** Escalate to: SLT Recorded with DSL
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email and communication tools after being warned • Continued unauthorised use of mobile phone/personal device after being warned • Continued use of unauthorised instant messaging / social networking sites, Games sites • Use of Filesharing software e.g. BitTorrent, for illegal downloading • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not notifying a member of staff of it	**Refer to Class teacher** Escalate to: **SLT** Removal of Internet access rights for a period / contact with parent/ Mobile phone not allowed in school for agreed period.

PUPIL	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Transmission of commercial or advertising material • Use of systems to circumvent schools online-safety tools such as VPN and proxy sites	**Refer to Class teacher / removal of Internet and/or online services access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions** **if inappropriate web material is accessed:** Ensure appropriate technical support filters the site and refer to DSL
Category D infringements	**Possible Sanctions:**
• Continued sending of emails or messages regarded as harassment or of a bullying nature Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent Sharing or requesting of images or content of a minor that would be considered sexual or inappropriate. • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	**Refer to Head Teacher/ DSL / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the service provider if appropriate. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, social networking etc. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Lack of due care resulting in infection or distribution of viruses or malware • Misuse of first level data security, e.g. sharing of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	**Referred to Head teacher / Governors;** **Other safeguarding actions:** ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as 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. *Escalate to: report to DSL/ LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on online-safety issues.

Appendix 9: 'What to do if?' Guide for staff

St Vincent's Catholic Primary School

Online Safety Policy

October 2017

Appendix 9

Guidance: What do we 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/DSL and decide whether to inform parents of any children who viewed the site.
3. Inform the school technician and ensure the site is filtered (CBC schools report to: **CBC Services**).

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. Notify DSL
4. Inform the school technician and ensure the site is filtered if need be.
5. Inform the LA.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify DSL and governing body (if appropriate).
4. Inform the school technician and ensure the site is filtered if need be.
5. Inform the LA.
6. In an extreme case where the material is of an illegal nature:
    a. Contact the local police and follow their advice.

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 (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams 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 (undertaken by Headteacher).
    - Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and DSL.

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 online-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify SLT and parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform DSL

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 and other agencies (child protection, Governing body etc).

The school may wish to 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 or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer (DSL) 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 and other agencies.

6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child

1. Report to and discuss with the named child protection officer (DSL) in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the IT technical body block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Inform the Headteacher

Contact the poster or page creator and discuss the issues in person

2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and online-safety officer (DSL).

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.