Our Lady and St Edward's Catholic Primary School

Online Safety Policy

Created March 2017
By C.Pickup Computing and Online Safety Leader
Updated July 2022
By C.Birch Computing and Online Safety Leader and consultation with C.Pickup Online Safety Leader

(updated and modified from previous ICT Security Framework Policy)

Our Lady and St Edward's Mission Statement

We are inspired by the teachings of Jesus Christ who is at the heart of all that we do.

Working in unity with our families, parish and community, we encourage and support the children to grow in faith and reach their full potential in a happy, caring and loving environment.

Developing and Reviewing this Policy

This online safety policy has been developed by;

- Cath Pickup – Computing and Online Safety Leader in consultation with Mrs K Woods (Headteacher and Designated Safeguarding Lead)

This online safety policy has been updated (March 2023) by;

- Charlotte Birch – Computing and Online Safety Leader in consultation with Mrs C Pickup (Online Safety Leader) and Mrs K Woods (Headteacher and Designated Safeguarding Lead)

Consultation will take place with;

- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Pupils

Policy Created: March 2017

Policy reviewed: March 2023

Policy to be reviewed: March 2024

This policy will be implemented and reviewed as appropriate by:

- Head teacher –Mrs K Woods
- Charlotte Birch – Computing and Online Safety Leader
- Cath Pickup – Online Safety Leader

Signed:

Head Teacher……………………………………………………………………………………

Signed…………………………………………………………….

Date …………………………………………………………….

Computing and Online Safety Leader…………………………………………………………….

Signed…………………………………………………………

Date ……………………………………………………………..

Online Safety Leader…………………………………………………………….

Signed…………………………………………………………

Date ……………………………………………………………..

Link Governor…………………………………………………………………………….

Signed…………………………………………………………

Date ……………………………………………………………..

Contents

Appendices

Section 1 – Our Lady and St Edward's Vision for Online Safety

1.1 Our Vision

At Our Lady and St Edward's we place high value on the use of modern and emerging technologies, not only to augment effective teaching with a range of inspirational and engaging approaches, but as an essential training platform for young people who will need specific ICT aptitudes and skills for a successful life, both personally and as members of the labour market. Effective use of ICT should enhance learning but also nurture creativity and technological thinking across the curriculum. Online safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. In order to make best use of the many educational and social benefits of new technologies, pupils at Our Lady and St Edward's need opportunities to explore the digital world, using multiple devices from multiple locations. It is now recognised that the online safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to the local and national guidelines on acceptable user policies. This Online Safety Policy details the way in which new and emerging technologies may and may not be used and identifies the sanctions for misuse. Learning platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.

1.2 Effective Practice

Online safety depends on effective practice at a number of levels and we achieve this at Our Lady and St Edward's by;

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Encouraging children to maximise the benefits and opportunities that technology has to offer and providing a diverse, balanced and relevant approach to the use of technology
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure network design and use
- Safe and secure broadband from a trusted provider including the effective management of web filtering and monitoring
- Ensuring children are equipped with the skills and knowledge to use technology appropriately and responsibly
- Teaching children and their families how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- Focused teaching of Online Safety as part of Relationships and Sex Education
- Communicating to all users in our school community why there is a need for an Online Safety Policy
- Communicating regularly with parents to reinforce the importance of children being safe online

1.3 Further Information

Keeping Children Safe in Education (Sept 2023)
https://assets.publishing.service.gov.uk/media/64f0a68ea78c5f000dc6f3b2/Keeping_children_safe_in_education_2023.pdf

Section 2 - Teaching and Learning

2.1 Why is internet use so important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 How does Internet Use Benefit Learning?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet. Teachers and pupils will have access to web sites offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others worldwide. In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DfE; receive up-to-date information and participate in government initiatives such as NGfL and the Virtual Teacher Centre.

2.3 Internet Use Will Enhance Learning

Developing effective practice in Internet use for teaching and learning is essential. Teachers will help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- The school reserves the right for teachers to use filtered website pages if they are appropriate in aiding teaching and learning (such as Youtube). All such sites will be thoroughly checked by the teacher and the Computing Subject Leader will be made aware before use so that they can be unblocked for the teacher account.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

2.4 Pupils will be taught how to evaluate the Internet Content.

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. Information received via the Internet, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.5 Preventing Extremism

The Internet is a powerful tool to target new people in order to indoctrinate them. Radicalisation is the promotion of increasingly extreme political, social or religious ideals. Extremism presents distorted views of history, politics or religion through persuasive narratives. Pupils, through rigorous online safety education and the measures described in the previous section of this policy (2.4), should be empowered to challenge ideas, think critically for themselves and take responsibility for their actions. Related issues will be considered in the context of a balanced PSHE curriculum. All members of staff will undertake Prevent training each year. Evidence of this yearly training is held by N. Kippax.

Section 3 – Responsibilities

3.1 Online Champions

All members of staff in school are expected to take responsibility for maintaining the safety of young people through a duty of care, and this includes safe and appropriate use of technology. However, in addition to this, the school has named Online Safety Champions.

The Computing Subject Leader, Miss Charlotte Birch, Online Safety Leader, Mrs Cath Pickup and Mrs Karen Woods (Headteacher and Designated Safeguarding Lead) are the main points of contact for online safety related issues and incidents. Both Charlotte Birch and Cath Pickup are part of the Senior Leadership Team.

Responsibilities include;

- Operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an online safety incident occur.
- Ensuring all Online Safety Incidents are logged by staff through CPOMS. KW and KOD (as DSL) to have access to this log at all times.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging online advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- To ensure a co-ordinated approach across relevant safeguarding areas with other safeguarding leads.

3.2 Headteacher

- The Head teacher and another member of the Senior Leadership Team (The Deputy Head who is also a DSL) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See appendix 8)
- The Head teacher and Senior Leaders are responsible for ensuring that the online safety leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

3.3 Technical Staff

- Technical support is provided by EasyTech NW Ltd
- Meets regularly with the Computing/ Online Safety Leader to discuss online safety issues.
- The technical staff are aware of the Online Safety Policy and AUP.
- Ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensures that the school meets required online safety technical requirements and any Local Authority / other relevant body online safety policy or guidance applies.
- Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

3.4 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governor panel receiving regular information about online incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor: **Mr A Metcalf**

- The role of the online safety Governor will include:
- Regular meetings with the online safety leader
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs

- Reporting to relevant Governors / Board / committee meeting

3.5 Teachers and Support Staff

- Teaching and support staff are responsible for ensuring that:
- they have an up to date awareness of online safety and current trends
- they have an awareness of the current online safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problems to the Head teacher or the Online Safety Leader
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure pupils in their care understand and follow the Online Safety Policy and Acceptable Use Policies when using technology and online communication methods.
- Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement school rules of acceptable use with regard to these devices
- in lessons, where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

3.6 Designated Safeguarding Lead

The DSL should be trained in online safety issues and be aware of current trend/ policies for Internet misuse and serious child protection / safeguarding issues that may arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

3.7 Pupils

- responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and forms of collaborating online. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.8 Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Our Lady and St Edward's will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, our website and information about national / local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of different technologies

Section 4 – Managing Internet Access

4.1 Appropriate and Safe Access to the Internet

The Internet is freely available to any person wishing to send e-mail or publish a website. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher, and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our Internet is provided by BT Lancashire Services and has a 'firewall' filtering system intended to prevent access to inappropriate material (Netsweeper)
- Children using the Internet during lesson time will be supervised by an adult at all times
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that children are using the agreed search engines and terms.
- Pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others. Each class has a class email which is the teachers' responsibility. Individual email can be accessed through the 'Purple Mash' VLE however only pupils and staff within school can be emailed and emails have to be checked before being sent.
- Agreed Online Safety Rules, created in consultation with upper KS2 children, are displayed in every classroom.
- The Computing Subject Leader will monitor the effectiveness of the Internet access strategies through communication with all members of staff.
- The Headteacher and Computing Subject Leader will ensure that the policy is implemented effectively.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LEA, our I.S.P. (Internet Service Provider) and the DfE.

4.2 Reporting Incidents

In the event that an online safety incident occurs that contravenes the online safety policy or agreed AUP's, it is important that the protocol below will be followed. It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged on CPOMs (in line with the school safe guarding policy). A most important element of our online rules is that pupils will be taught to tell an adult immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels;

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers/guardians to resolve any issues.
- If pupils discover unsuitable sites they will be taught to report it to an adult in school. The adult will then inform the Computing / Online Safety Leaders and make a log of the incident using CPOMS. The Computing leader will report the URL (address) and content to LGFL
- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use, which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use email facilities and fail to follow the rules they have been taught, then sanctions consistent with the Behaviour Policy will be applied. This will involve informing parents/carers/guardians. Teachers may also consider whether access to the Internet may be denied for a period of time.

Online Safety incidents that occur outside of school but are brought to the attention of teachers in school either through pupils or parents, will be dealt with appropriately. All parents of children involved will be informed and staff will support children in school. These incidents are logged using CPOMS.

4.3 Ilegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 8) Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk).They are licensed to investigate – schools are not.

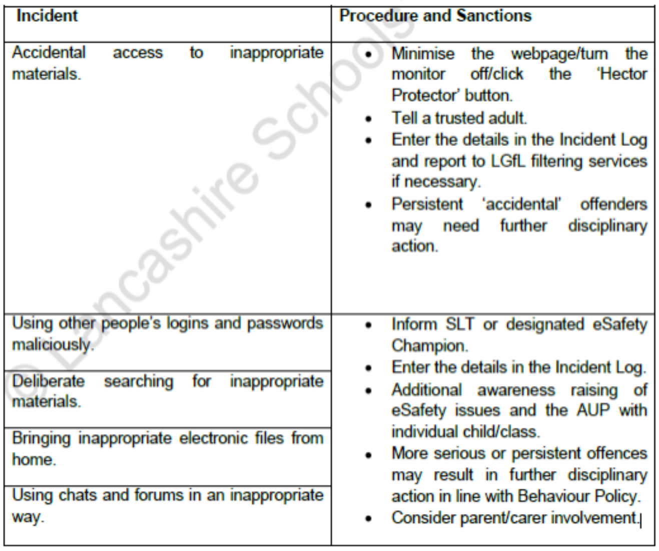
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk.

4.4 Inappropriate Use and Sanctions

It is important that any incidents are dealt with quickly and actions are proportionate to the offence. If the guidelines or AUPs are breached, or suspected of being breached, the Headteacher should be notified if appropriate. Some examples of inappropriate incidents are listed below with possible sanctions, although this will ultimately be at the discretion of the Headteacher. All incidents should be logged using CPOMS.



Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Where staff are suspected of contravening the AUP, this should be reported to the Headteacher who will take appropriate steps in accordance with the school's discipline policy. Our Lady and St Edward's uses a holistic approach to online safety, and as such all staff are responsible for dealing with online safety incidents appropriately at class level. The online champion should be notified of any online safety incidents, who will then liaise with the Headteacher as appropriate. All online safety incidents will be logged on CPOMS. DSL can view all incidents logged on CPOMS at any time. These will be monitored regularly with action plans put in place as necessary to avoid further incidents where possible. School will use the 'eSafety Incident/ Escalation Procedures' document (See Appendix 8) as a framework for responding to incidents.

4.5 Security and Data Management

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

- The IT technician will up-date virus protection regularly (Sophus provided by LCC), and both the technician and Computing leader will keep up-to-date with IT news, developments and work with the Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

ICT security is a complex subject that involves all technology users dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire ICT Security Framework (published 2005) has been consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Key information is held on the school's Server accessed through password protection.
- As part of the Induction process for new staff or procedures for staff changing roles individuals are updated on the location of data specifically required for their role.
- Induction also confirms the sensitive and confidential nature of all data held.
- Any data taken from the school environment is held on password protected or encrypted devices.
- All staff are required to read, sign and return the school's Acceptable Use Policy.
- Staff understand that they should only use approved means to access, store and dispose of confidential data.
- Remote access to school data is only done by the Headteacher and Bursar and is password secure.
- Expectations regarding the use of mobile devices in school are made clear in the, Safeguarding Policy and the AUP's. We recommend that staff password protect their own mobile devices.
- Data stored on the administration server is backed up BT Lancashire Services as part of a subscription service. This is currently done nightly.

Section 5 - Infrastructure and Technology

5.1 Network

Our Lady and St Edward's aims to ensure that our infrastructure and network is as safe and secure as possible. This section of the policy defines the policies and procedures in place to safeguard users. The ICT network at OLSE is protected by a broadband filter. Our internet provider is **BT Lancashire Services** and out filtering service is provided by **Netsweeper**. However, should unsuitable content not be detected by this filter, children are educated to minimise the screen and inform an adult immediately. Staff will subsequently report the URL of inappropriate content to LGFL via the online reporting form which is available in such an event. The school is also able to immediately block websites via the use of this filter and attempts to access any inappropriate content is flagged. This enables the school to block inappropriate material immediately at school level.

5.2 Pupil Access

Children should only access the internet using school computers when supervised by a trusted adult.

5.4 Passwords:

- Staff have passwords to access the teacher part of the server and these must not be shared.
- Only staff user profiles will be able to make administrative changes to programmes and access the teachers' area of the network.
- Pupils will use a single, simple year group password for access to the school network. This profile will have limited privileges, with any changes reset upon logging out.
- Passwords should be changed at least once every academic year.

5.4 Software/hardware:

- All software used in school must be owned by the school, or by staff at the school, with appropriate user licenses used.
- Licenses should be kept centrally in the designated License folder by the Bursar.
- App licences for volume app purchases are logged within the school iTunes account.
- Where appropriate, any annual subscriptions should be renewed in good time. This is the responsibility of the Computing Subject Leader and Bursar.
- All computing equipment and software is audited every 2 years at the same time as the computing policy is reviewed.
- Any additional equipment required will be budgeted for in the annual Action Plan.
- Software is installed on systems by the ICT technician.

5.5 Managing the Network and Technical Support:

The school network is managed by Easy Tech LTD through a service level agreement. Easy Tech LTD are responsible for all aspects of network technical support and maintenance. Easy Tech visit the school once a week to perform maintenance and solve any issues. The following procedures are to be followed to ensure the network and all data remains secure:

- Servers, wireless systems and cabling are securely located and physical access restricted .
- Wireless devices must have security enabled .
- The wireless network is accessible only through a secure password, available only to members of staff.
- The SLT and the Computing Subject Leader are responsible for managing the security of the school network.
- The safety and security of the network is reviewed by Easy Tech LTD Solutions on each maintenance visit.
- The Computing Subject Leader will also ensure measures are in place to maintain the security of the network where new risks arise.
- Easy Tech LTD ensure that all computers are configured to receive all necessary updates and patches.
- There is a separate password for pupils and staff, who each have their own user profile.
- Only staff will have permissions to change their system profile and install necessary software.
- The overall network administrator password is available only to the Computing Subject Leader and the Headteacher.
- Staff and pupils log out of computers at the end of each session.
- If any users suspect a breach of network security, they should inform the Computing/Online Safety Leader immediately. Easy Tech LTD will be contacted for assistance.
- Removable storage devices are permitted to be used in school, however if they contain any sensitive data they must be in password-protected or encrypted folders.
- Removable storage devices are to be regularly checked for virus and this is the responsibility of the adult user.
- Where school laptops are loaned to teachers, these may be used for acceptable personal use only. Further guidance can be found in the 'Staff Use of Internet' AUP.

- Easy Tech LTD are aware of all requirements and standards regarding online safety.
- The Computing Subject Leader, Online Safety Leaders and Headteacher are responsible for liaising with and managing the technical support staff from Easy Tech LTD when using school computers.
- Logs are kept each visit to ensure essential maintenance has taken place.

5.6 Filtering and virus protection:
Sophos Anti-Virus software is used on all school computers. This is updated regularly automatically by Easy Tech LTD. Any laptops or other devices that access the network must have up-to-date Anti-Virus software.
In accordance with;
Keeping Children Safe in Education (Sept 2023)
https://assets.publishing.service.gov.uk/media/64f0a68ea78c5f000dc6f3b2/Keeping_children_safe_in_education_2023.pdf

The school know that Netsweeper Systems is an appropriate filtering system that blocks illegal content and are IWF (Internet Watch Foundation) members. We undertake yearly checks using the South West Grid for Learning filter test.

We have some control to permit access to specific content carefully checked by the class teacher and agreed by the Computing Subject Leader

Our Lady and St Edward's currently assess our risk as low therefore the monitoring approach will be physical. Our current practice of having adult supervision of Internet use means screen activity can be monitored for inappropriate use. Staff are aware of safe practice and understand the need to report any inappropriate use of the internet. The Online Safety Leaders will keep up to date with monitoring advice and adjust school practice accordingly.

Section 6 – Communication and Publishing

6.1 Email

Pupils will learn how to use e-mail and be taught e-mail conventions, however children will not be given personal e-mail addresses to use in school other than the internal use of the email section on 'Purple Mash,' which is moderated by class teachers. Although children have a google email to access the school Chromebooks, the Gmail is disabled on pupil accounts so they cannot access emails. Staff will use school e-mail address 'Office 365' to communicate with others, to request information and to share information. Each class has an e-mail address for shared class projects using Office 365.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- All staff will use Office 365 e-mail, which is the Lancashire preferred school email system.
- The Lancashire Grid for Learning Service will reduce the amount of SPAM and any SPAM incidents should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school. Personal email accounts should not be checked in the presence of children, or connected to the overhead projectors/whiteboards.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- Any communication needed about children via e-mail will be done through initials and for appropriate reasons.
- The forwarding of chain letters is not permitted.

- Pupils will be taught that they must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.
- Teachers will endeavour to ensure that these rules remain uppermost in the pupil's minds when as they monitor children using e-mail.
- Pupils may send e-mail from a class e-mail account as part of planned lessons but will not be given individual e-mail accounts;
- Pupils will have the e-mail messages they compose checked by a member of staff before sending them.
- Pupils will not have individual access to the class e-mail account.
- Pupils will have individual access to 'Purple Mash' VLE e-mail where they can e-mail internally and be taught e-mailing skills, which is monitored by staff.

6.2 Published Content and the School Website

The school website is a valuable resource. It celebrates pupils' work, promotes the school and publishes resources for projects and homework. The website reflects the school's ethos, information is accurately and well-presented and personal security is not compromised. Publication of information is considered from a security viewpoint as web sites can be accessed by anyone on the Internet.

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- All teachers have been trained in publishing on the website and are responsible for ensuring content is appropriate on class pages.
- The head, deputy head, bursar and Computing Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website is a fundamental place for communicating online safety messages to pupils and parents/carers, and has a dedicated online safety section.
- All materials on the website shall adhere to copyright restrictions. - Sensitive documents should only be available in 'read-only' formats, such as PDFs.

6.3 Pupils' Images and Work

Photographs that include pupils add a liveliness and interest to the school's website that is difficult to achieve in any other way. Nevertheless the security of staff and pupils must come first. A check should be made that pupils in photographs are appropriately clothed.

- Photographs of pupils will not be published without parental permission.
- Photographs that include pupils will be selected carefully and will only enable individual pupils to be clearly identified when parental permission has been gained.
- Pupils' full names will not be used anywhere on the website.
- Every September all parents are asked to sign a consent form for use of their child's photo.
- The school will keep a record of all pupils who are not permitted to have their photos or work published to the web. The record will be kept up-to-date, for instance a child or family joins the school.

6.4 Cloud Storage

Our Lady and St Edward's considers carefully where data is stored. Please see cloud storage policy.

6.5 Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others. To prevent our pupils accessing inappropriate social networking sites, the following procedures will be put in place:

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught to never to give out personal details of any kind which may identify them 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 and parents will be advised that the use of social networks is inappropriate for primary aged pupils and that they have minimum age restrictions.
- When blogging in school children's names and pictures will not appear together.
- Blogging will be supervised at all times.
- Comments and responses will be monitored and checked before publishing.

Our Lady and St Edward's considers the following to be an acceptable use of social media by staff;

- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, or details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. –
- If a Social Network site is used by staff, details must not be shared with pupils and privacy settings be set at maximum.
- Staff should be aware that 'friends of friends' may be able to view 'tagged' photographs/comments, which may bring the individual member of staff or the school into disrepute.
- Comments made and photographs posted reflect the professional reputation of the school, and once posted cannot be un-done.
- Pupils must never be added as 'friends' by staff. If a pupil persists in making friend requests, it is necessary to log the incident in the online log and report to the online safety champion, who will deal with the matter appropriately.
- No pupils under the age of 13 should be using Facebook. However, it is known that a large proportion of children under this age do use this Social Network. It is the school's responsibility to ensure that children are educated on the safe use of all Social Networks.
- Where is it known, or reported, that a child under the age of 13 is using Facebook or other equivalent social media site, an information letter will be sent to parents/carers. –
- All OLSE pupils will receive regular teaching and guidance in the safe use of the Internet, Emailing, Social Networking and Cyber-bullying. We have an Online Safety Curriculum using Project Evolve and all objectives are taken from Education for a Connected World. Key messages and learning will be delivered during specific computing cyber-bullying awareness lessons, and re-enforced in class and whole school assemblies. Regular reminders will be used in class when children are accessing the Internet. Teachers can select from a wide range of resources to support this learning, including;
  - www.kidsmart.org.uk
  - www.childnet.com
  - www.lancsngfl.ac.uk
  - thinkuknow.co.uk
  - www.bbc.co.uk/cbbc/topics/stay-safe

These URL's will be added to the school website for pupil and family access away from school.

6.6 Video Conferencing

At Our Lady and St Edward's the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Approval must be sought in advance from the Headteacher prior to video-conferencing taking place.
- Only secure, approved programs to be used for video conferencing.
- All pupils will be supervised when using video conferencing.
- Additional written consent should be sought for the use of video conferencing from parents/carers.
- It should be made clear to the receiver that no recordings may be taken without permission.
- Staff know how to terminate the video conference at any time.

Section 7 – Mobile Technologies

The use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is commonplace in school. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication. Here at Our Lady and St Edward' each classroom has a teacher iPad and 6 mini iPads. We also have a set of 16 iPads which can be used by classes. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.1 Mobile phones

- Staff are not allowed to use mobile phones in classrooms. These are to be kept in a secure location, at the staff member's discretion and can be used in the staff room at lunchtime or in classrooms after the school day has ended and children have left the site.
- Staff are encourage to password protect their personal mobile phone.
- In exceptional circumstances, with the Head teacher's permission staff can access their mobile phone during the school day.
- In the event of a staff member needing to be contactable the main school phone can be used.
- Children are not permitted to bring mobile phones into school unless this has been agreed between staff and parents for a specific purpose. In this instance the pupil's/family's phone will be stored at the school office to be returned when necessary (the end of the school day, or agreed time).
- If a mobile phone is brought into school by a pupil without permission it will be confiscated immediately and returned to the family. The child may face a consequence in line with the school Behaviour Policy.
- Staff are encouraged to use their mobile phone as a safety control measure during school trips. However, school devices (cameras and iPads) are to be used for photography.
- Through online safety awareness training and the computing curriculum staff and pupils are made aware of issues around cyber-bullying.

7.2 Cameras and Recording Devices

The use of cameras and sound recording devices offer substantial benefits to education but equally present school with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites. Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998).

- No cameras or other recording devices (including iPads) are to be taken from the school site for personal use.
- No personal cameras can be used in school, this includes devices with a built in camera such as a mobile phone.

7.3 Consent and Purpose

- Each year school asks parents to complete an Image Consent Form. These are collated and permissions communicated to class teachers and club leaders in school.
- The consent of adult staff members to have their photographs taken is assumed unless told otherwise

- The purpose of any photography is always communicated to those involved (ie. assessment, display, celebration, website, media).
- Consent forms include permission to store images.
- Further consent will be sought if the school intends to use a photograph after a pupil has left.
- Visitors must ask consent to take photographs and act in accordance with relevant codes of conduct.

7.4 Taking Photographs / Video

- All adults in school are permitted to take photographs for school purposes at the direction of class teachers using school owned equipment.
- If a child does not want to be photographed their choice will be respected. Children are not filmed or photographed when this might cause embarrassment, distress or if the child is injured.
- In addition, photography that could be misinterpreted is also avoided. E.g. close up shots of children participating in PE activities.
- Teachers will take a range of photographs representing many or all class members. - Group shots, with a background context are favoured.

7.5 Parents Taking Photographs/Videos

In line with our Safeguarding policy, Parents are asked not to take photographs during performances due to distraction. Under the Data Protection Act (1998), parents are entitled to take photographs of their own children on the provision that the images are for their own use, e.g. at sports day. At these events parents are reminded that images and video cannot be published on social networking sites.

7.6 Storage of Photographs / Video

- All images are stored on password protected school equipment. On rare occasions images may be taken off site for the purposes of producing a display; in these instances they are kept on the same password protected equipment and returned to school.
- Staff do not store images on personal equipment.
- Access to equipment containing images is managed and monitored by class teachers. It is also the class teachers' responsibility to delete and dispose of digital and printed video/images.
- Emailed images are sent within the school's secure email system.
- Full names are never published with images.
- All photos to be saved in the Staff Resources shared area on the server in a folder named photos. They need to be deleted from the device once uploaded which should be at least weekly.
- Photos will be deleted from the server after seven years although a small number of photos may be kept for curriculum evidence and to commemorate special events such as the bi-annual art exhibition.

Section 8 - Education and Training

8.1 Acceptable Use Policies

Our Acceptable Use Policies are intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

The school has the following AUP's in place (see appendices):

- Computing AUP – Staff and Governor Agreement
- Computing AUP – Supply Teacher and Visitors/Guests Agreement
- Computing AUP – Pupils Agreement/Online Safety Rules

- Computing AUP – Parent's letter

The school promotes online safety rules with ICT in teaching. These are displayed wherever computers are used in school.

Education and training are essential components of effective online safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online safety is embedded within the curriculum and advantages taken of new opportunities to promote online safety.

8.2 Online Safety Across the Curriculum

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of online safety risk (as mentioned by OFSTED, 2013) that school must be aware of and consider are:

Area of Risk	Examples of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	-Children need to be taught that not all content is appropriate or from a reliable source. - Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. - Lifestyle websites, for example proanorexia/ self-harm/suicide sites. - Hate sites. - Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	- Grooming - Cyberbullying in all forms - Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	-Privacy issues, including disclosure of personal information, digital footprint and online reputation - Health and well-being - amount of time spent online (internet or gaming). - Sexting (sending and receiving of personally intimate images). - Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Online safety is embedded in all ICT curriculum areas, in particular the strands of Information Technology and Digital Literacy. The school also participates in the annual 'Safer Internet Week', with specific teaching and discussion of online issues. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. The school online safety rules are regularly referenced during computing sessions. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology. Pupils are also reminded of relevant legislation regarding the Internet, such as copyright implications. Pupils are taught during Digital Research units to critically evaluate materials and content. This is reinforced in all other cross-curricular ICT sessions.

Online safety rules are displayed wherever computers are used in school. This is differentiated by key stage (see Appendices).

8.3 Raising Staff Awareness

- All staff, upon starting work at the school, are required to agree to the school's AUP's and are provided with a copy of the online safety policy and key staff guidelines, which includes personal safeguarding.
- Staff training updates for online safety will be delivered as necessary, with a minimum of once per academic year.
- All training and advice will be delivered by the, The Computing and Online Safety Leader.
- The Online Safety Leader will keep aware of updates to online safety guidelines and receive external training as necessary.
- All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting online safety whilst using ICT.

8.4 Raising Pupil Awareness

- Online safety rules will be displayed in all classrooms.
- Pupils will be informed that network and internet use will be monitored.
- An online safety module is included in all years of the Lancashire Creative Curriculum.
- Additional reference will be made to online safety during Online Safety day in February and during Anti Bullying week in November.
- Online safety rules are regularly referenced during all computing sessions.

8.5 Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

At Our Lady and St Edward's we offer regular opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies.

This takes place through:

- School newsletters.
- A dedicated area on the school website, which promotes external online resources and online materials.
- Parents online safety awareness sessions and advice available from the online safety champions.
- We will communicate any online safety concerns highlighted from other sources such as the media.

8.6 Raising Governor Awareness

- Governors are kept updated on arising online matters through the Annual Report to Governors for Computing and Online Safety.
- Governors also review and agree the Online Safety Policy annually, following discussion with the Online Safety Champions.
- The online safety log book is also available to the Governors at any time.
- Governors sign the staff AUP

Our Lady and St Edward's is committed to keeping children and staff safe online.

APPENDIX 1

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the school's Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing Online Safety as part of your child's learning, we will also be holding Parental Online Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the Lancsngfl Online Safety website;
http://www.lancsngfl.ac.uk/onlinesafety

Yours sincerely,

Mrs C Pickup

Appendix 2

PARENTAL CONSENT FORM – PHOTOGRAPHIC, VIDEO and INTERNET

At Our Lady and St Edward's we love to share the activities and achievements of our children with parents and the wider community. Photographs and videos are a way to share these experiences with you and the images and recordings we take during activities in school may be used on our website http://www.ourlady-st-edwards.lancs.sch.uk, in school publications such as newsletters or on display boards in school.

Also, our school may occasionally be visited by the media who will take photographs or film footage of a high profile event, or to celebrate a particular achievement. Pupils will often appear in these images, which may appear in local or national press and websites or on televised news programmes.
In order that we can protect your child's interest and to comply with the Data Protection Act 1998, **please read the Conditions of Use attached before answering questions below and signing and dating this form. Please return the completed form (one for EACH child) to school as soon as possible.**
(please tick)

Images and Video	YES	NO
Do you agree to photographs/videos of your child being taken by authorised staff within the school?		
Do you agree to photographs/videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events?		
May we use your child's image in printed school publications and for digital display purposes within school?		
May we use your child's image on our school's online publications e.g. website / blog / Purple Mash?		
May we record your child on video to support learning?		
May we allow your child to appear in the media as part of school's involvement in an event?		
Digital Content Storage		
May we store digital content created by your child on our server and the school's secure cloud storage platforms.		
Internet Permission		
I grant permission for my child to use the Internet for Independent work. I understand that some material on the internet may be undesirable or objectionable and that Our Lady and St Edward's is taking all reasonable precautions to stop pupils gaining access to this material. I support the Internet and Online Safety rules set by Our Lady and St Edward's as written in the children's Acceptable Use Policy		

I have read and understand the conditions of use provided with this form.

Child's Name ____ Class ___________

Parent's or Guardian's Signature____

Name (capital letters please) ____

Date _________________________

Conditions of Use

1. This form is valid for this academic year 2016/2017. (edit as appropriate annually)

2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.

4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.

7. 3rd Parties may include other children's parents or relatives e.g. attending sports day

8. Images/videos will be stored according to Data Protection legislation and only used by authorised personnel.

9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

10. Digital content refers to the increasing amount of content children have created on iPads or Computers. Content may be saved on the school server or in virtual learning environments such as Purple Mash or online cloud storage applications such as Purple Mash/ Dropbox or SeeSaw. Purple Mash is UK based and Dropbox and See Saw are USA based. The school follows a strict policy regarding online content storage. No images of your child or identifiable content will be saved in cloud storage.

Notes on Use of Images by the Media
If you give permission for your child's image to be used by the media then you should be aware that:
1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).
3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

If you have any questions regarding the above please do not hesitate to contact Mrs Cath Pickup, Computing and Online Safety Leader.

APPENDIX 3
Our Lady and St Edward's – ICT Acceptable Use Policy (AUP)
Staff and Governors Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff are aware of their individual responsibilities when using technology. All staff members are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Karen Woods (Headteacher).

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with pupils and other adults are appropriate.
8. I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)
9. I will not install any hardware or software without the prior permission of the Computing Subject Leader, Cath Pickup
10. I will ensure that personal data (including data held on SIM systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
12. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17 I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
21. I will undertake Prevent training provided by the school and understand that I have the duty to report any online activities that could be linked to terrorist activity or radicalisation.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.
Signature ____ Date ________________________
Full Name ____ (PRINT)
Position/Role ____

APPENDIX 4

Our Lady and St Edward's – ICT Acceptable Use Policy (AUP)
Staff Agreement
Supply teachers and Visitors/Guests Agreement

For use with any adult working in the school, for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

3. I will not use any external device to access the school’s network e.g. pen drive.

4. I will respect copyright and intellectual property rights.

5. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

6. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

7. I will not install any hardware or software onto any school system.

8. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

9. I understand that the use of personal mobile phones is not permitted in classrooms or any other room where children may be present.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ____ Date

Full Name

____ (PRINT)

Position/Role ____

APPENDIX 5

Our Lady and St Edward’s – ICT Acceptable Use Policy (AUP)
Children

These rules reflect the content of our school’s Online Safety Policy . It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. I will only use ICT (e.g. computers, i-Pads etc) in school for school purposes.

2. I will not bring equipment such as mobile phone, mobile games consoles or tablets into school unless specifically asked by my teacher.

3. I will only use the Internet and/or online tools when a trusted adult is present.

4. I will only use my class e-mail address or my own Purple Mash email address when emailing.

5. I will not deliberately look for, save or send anything that could be unpleasant, nasty or embarrassing to anyone including me.

6. I will not deliberately bring in inappropriate electronic materials from home e.g video clips/films that aren't appropriate for my age.

7. I will not deliberately look for, or access inappropriate websites.

8. If I accidentally find anything inappropriate or feel uncomfortable I will tell my teacher immediately.

9. I will only communicate online with people a trusted adult has approved.

10. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

11. I will not give out my own, or others', details such as names, phone numbers or home addresses.

12. I will not tell other people my ICT passwords except a trusted adult.

13. I will not arrange to meet anyone that I have met online.

14. I will only open/delete my own files at my teacher's request.

15. I will not attempt to download or install anything on to the school network without permission.

16. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

17. I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety.

18. I understand that if I don't follow the rules that the school may take disciplinary steps in line with the school's Behaviour Policy. This could mean being given a warning or even banned from using certain ICT equipment for a while if I did something very serious.

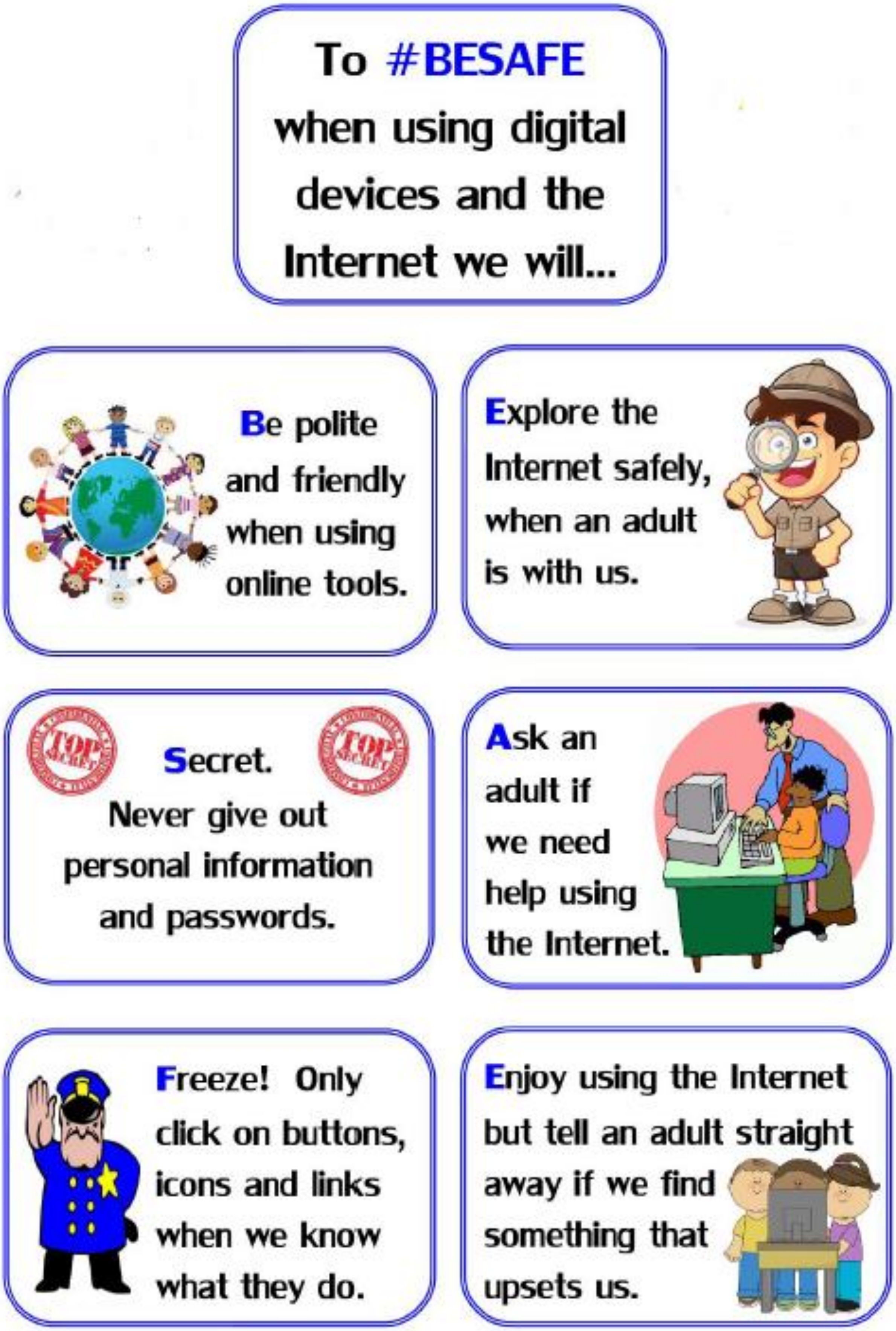
We have discussed this Acceptable Use Policy and my child _________________________________ agrees to follow the online safety rules and to support the safe use of ICT at Our Lady and St Edward's .

Parent /Carer Name (Print) ……………………………………………………………………………………….

Parent /Carer (Signature) ……………………………………………………………………. …………………………..
Class ………………………………………………. Date………………………………………………………………….

APPENDIX 6

EYFS KS1 Online Safety Rules



To #BESAFE when using digital devices and the Internet we will...

Be polite and friendly when using online tools.

Explore the Internet safely, when an adult is with us.

Secret. Never give out personal information and passwords.

Ask an adult if we need help using the Internet.

Freeze! Only click on buttons, icons and links when we know what they do.

Enjoy using the Internet but tell an adult straight away if we find something that upsets us.

Appendix 7

Online Safety Rules KS2

To #BESAFE when using digital devices and the Internet we will...

Be polite and friendly when communicating using online tools and digital devices.

Explore the Internet safely, with the permission of an adult and when an adult is present.

Secret.
Never give out our own or others' personal information and passwords; be careful with the information that we share online.

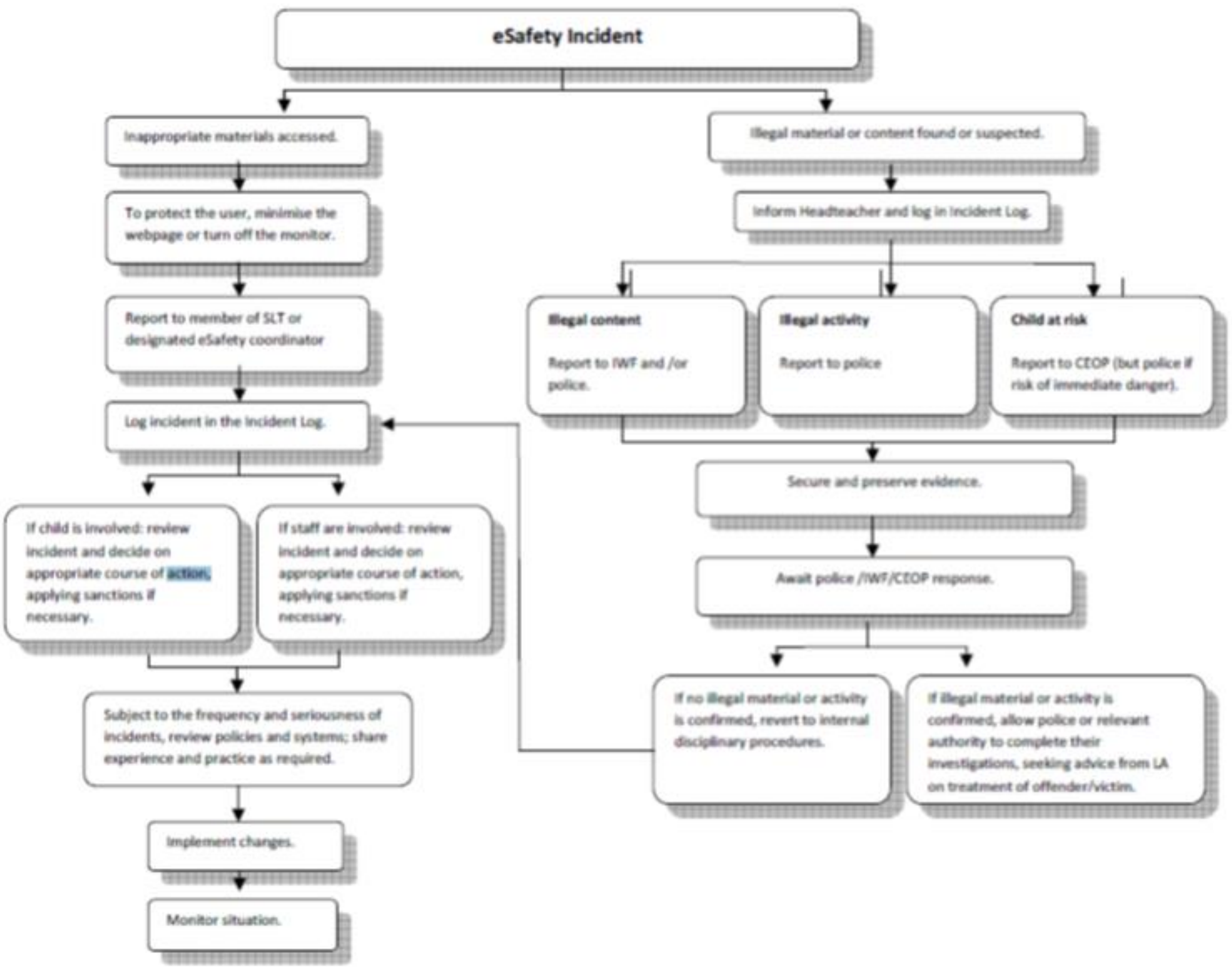
Approved.
Only use Apps, programs and digital content that has been approved by an adult.

Freeze!
Immediately minimise any page containing content we are uncomfortable with and tell an adult.

Enjoy using the Internet and digital devices and make sure that others can do the same.

APPENDIX 8

· Responding to eSafety Incident/ Escalation Procedures



eSafety Incident

Inappropriate materials accessed.

To protect the user, minimise the webpage or turn off the monitor.

Report to member of SLT or designated eSafety coordinator

Log incident in the incident Log.

If child is involved: review incident and decide on appropriate course of action, applying sanctions if necessary.

If staff are involved: review incident and decide on appropriate course of action, applying sanctions if necessary.

Subject to the frequency and seriousness of incidents, review policies and systems; share experience and practice as required.

Implement changes.

Monitor situation.

Illegal material or content found or suspected.

Inform Headteacher and log in Incident Log.

Illegal content

Report to IWF and /or police.

Illegal activity

Report to police

Child at risk

Report to CEOP (but police if risk of immediate danger).

Secure and preserve evidence.

Await police /IWF/CEOP response.

If no illegal material or activity is confirmed, revert to internal disciplinary procedures.

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA on treatment of offender/victim.

Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp

LCC Schools' eSafety Lead

Lancashire Schools' ICT Centre
(01257) 516360
info@ict.lancsngfl.ac.uk

Securing and Preserving Evidence – Guidance Notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system).
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
- Make a note of the date / time of the incident along with relevant summary details.
- Contact your School's Neighbourhood Policing Team for further advice.