



St John with St Augustine Primary School

Online Policy

Online encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing such as online 'blogs' and online forums including Twitter and Facebook. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's Online Safety policy operates in conjunction with other policies including those for Child Protection, Pupil Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

The policy has been discussed and approved by staff and governors and is based on the recent recommendations by Lancashire County Council (2017). The purpose of these measures is to protect users, the school and LCC and to make the use of online technologies a safer and more enjoyable experience.

Good Practice Regarding e-Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Cleo Network including the effective management of Lightspeed Filtering Web filtering.
- National Education Network standards and specifications.

Introduction

Writing and reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for all curricular subjects, behaviour, anti-bullying, cyber bullying and child protection.

- St John with St Augustine PS Online Safety co-ordinator Mr Hollinshead & Miss Martin (DSL)
- Our Online Safety Policy has been written by the school, building on the Lancashire Online Safety Policy and government guidance and approved by governors
- The Online Safety Policy and its implementation will be reviewed annually unless further guidance is received from LA.

The School's Online Safety Co-ordinator

The Online Safety Co-ordinator is the main point of contact for Online Safety related issues and incidents. The role of the Online Safety Co-ordinator includes:

- Having 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 an Online Safety Incident Log is appropriately maintained and regularly reviewed. APPENDIX 11 – Online Safety Incident Log
- 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 Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated DSLs to ensure a coordinated approach across relevant safeguarding areas.

Some of the above responsibilities may be delegated to appropriate members of staff.

Security and Data Management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire ICT Security Framework (published 2005) should be 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.

All data in school must be kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy–

APPENDIX 4 –ICT Acceptable Use Policy (AUP) – Staff and Governor Agreement

APPENDIX 5- ICT Acceptable Use Policy (AUP) – Supply Teachers and Visitors/Guests Agreement

Depending on your role in school you will have access to different network drives.

The Computing Co-ordinator has access to all areas.

Supply teachers only have access to the Shared drive so Flipcharts must be saved in their supply teachers folder. Always use the supply teacher login for supply teachers.

Parent's workshop and other visiting groups have no access to any drives and are unable to save onto computers.

Data on the curricular and admin system is backed up locally daily by BT connect remote backup BT connect monitors the back-up of data and deletes older back-ups when they are no longer required, all data is encrypted.

Staff are permitted to use pen drives and other similar devices to transfer none personal information such as lesson plans and resources for use in school and at home.

Assessment data, such as 'Trackers', are stored on the OneDrive drive on the school Login ID, access to which is restricted by password to Teaching staff only. Staff are instructed not to store electronic copies of this data at home.

All user accounts are password protected and staff have to change their password regularly.

There is currently no remote access to school servers from home but the OneDrive is accessible using login ID and password.

We have one wireless network in school which is secure:

1. Staff wireless

The Use of Mobile Devices

School use of mobile devices, including laptops, tablets, iPads, cameras and games consoles is becoming more commonplace. 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.

Mobile phones

Mobile phones can present a variety of challenges if not used appropriately. Smart phones can upload pictures onto cloud storage so even if you delete picture from phones memory, it's still stored on cloud. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available.

In order to balance the benefits of mobile phones alongside the possible issues they can create, the school has a number of guidelines in place:

- Staff are not permitted to use mobile phones in school during contracted school hours unless with the permission of the Head teacher.
- Children are not permitted to have mobile phones in school. They may store these securely in the office but **MUST** be switched off.
- Parents are asked not to use mobile phones inside the school premises or outside when a lesson is taking place. A notice is on display to remind visitors of the rule.
- Staff are responsible for the security of their own belongings
- Staff **MUST** store their mobile phones in 'silent' mode or off during contracted hours and this cannot be on their person.

- Images of children video or audio must not be recorded on personal mobile phones.

The Misuse of Mobile Phones

Mobile phones are one potential source of cyber bullying. The issue of cyber bullying is discussed with the children as part of the online safety/PSHE curriculum. The school reserves the right to confiscate a phone or device if there is good reason to believe that it is being used to contravene the school's behaviour policy. In the event of such action being required the head teacher or a member of the SLT would be informed and involved in the process and parents would be informed of the reasons for the action. Staff are asked to be vigilant in monitoring visitors for any covert use of mobile phones or cameras and to report any concerns to the head teacher.

Use of digital media (cameras and recording devices)

The use of cameras and sound recording devices offer substantial benefits to education but equally present schools 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).

Consent and Purpose

- Written consent is collected from parents for photographs of their children to be taken or used. Permission is given through a general written consent form issued to all families
- Staff are informed of any children whose parents or guardians have not given their consent for their photographs to be taken or their images used in digital form by the school. These names can be found in the school office. It is the responsibility of staff to ensure that only images containing children whose parents or guardians have given permission are used by the school. Verbal consent is not considered acceptable.
- Images of staff or adults employed in the school will not be used without their written permission.
- It is made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties).
- Images of children should only be stored on the school class computers which are password protected and deleted once used.
- Parents are informed of the purposes for which images may be taken and used in the consent form e.g. displays, website, brochures, press and other external media.
- Images that at times may be displayed in public areas, e.g. the entrance hall, are subject to the same restrictions.

Taking Photographs / Video

- Teachers and Teaching Assistants are authorised to take images related to the curriculum.
- Photographs and videos are only taken using **school owned equipment**, including memory cards, digital tape and tablets. The use of personal equipment to take or store images is prohibited.
- When taking photographs and video the rights of an individual to refuse to be photographed are respected.
- Photographs must never show children who are distressed, injured or in a context that could be embarrassing or misinterpreted.
- Care is taken to ensure that individual children are not continually favoured when taking images.
- The subject of any film or photograph must be appropriately dressed and not participating in activities that could be misinterpreted e.g, particular care may be needed with the angle of shots for children engaged in PE activities.
- Certain locations are considered 'off limits' for taking photographs, e.g. toilets, cubicles, etc...
- Discretion must be applied with the use of close up shots as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

Parents Taking Photographs / Videos

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 a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

- Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.
- As it is virtually impossible for school to monitor parental pictures the school now publishes pictures on the school website after pictures are checked.
- Parents are reminded, in writing, that publishing images which include children other than their own or other adults on **Social Network** sites is not acceptable.

Storage of Photographs / Video

- Photographs are securely stored and should not be removed from the school environment unless for a specific purpose. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets.

- Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used
- Cloud storage is used for Ipads but checked and deleted regularly.
- Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices.
- Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted.
- Access to photographs / videos stored on school's equipment is restricted to school staff. The server allows data to be stored so that it is accessible either to all staff, teachers or pupils.
- Individual members of staff are responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed. The ICT Co-ordinator and IT manager have access to all areas of the network and can assist with the removal of data.
- Should a parent withdraw permission the class teacher is responsible for the removal and deletion of images and may be assisted by the ICT coordinator.
- Photographs sent electronically must be sent securely. This is done using staff accounts on the Lancashire e-mail system OFFICE 365..

Publication of Photographs / Videos

- Consent is needed from parents for publication of children's images, e.g. on a website.
- Photographs should only be published online to secure sites.
- Full names and / or other personal information should not accompany published images.

When publishing images

- Children's images taken in school should not be displayed on insecure sites e.g. personal social networking sites. Parents and staff are informed in writing of this. If such images are reported their immediate removal will be requested.
- Staff and children are made aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- All staff should recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites. Staff should ensure that personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

The Media, 3rd Parties and Copyright

- Visiting third parties within school are supervised at all times whilst in the school and are expected to comply with the Data Protection requirements in terms of taking, storage and transfer of images.
- The copyright for images taken by a 3rd party must be made clear beforehand and agreed by the school and parents before such images are used, eg in a local newspaper.
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, staff are expected to read and be familiar with read the terms and conditions of the web site. (You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions).

Communication technologies

School uses a variety of communication technologies, each of which carries various benefits and associated risks. All new technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the Online Safety Policy will be updated and all users made aware of the changes. The policy is reviewed annually.

Email

- The Lancashire Office 365 service is the preferred school email system.
- Staff should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the head teacher and access is required for professional purposes.
- E-mail accounts for children are organised as class accounts or computer, eg Year4. This ensures that children cannot be identified through an individual e-mail address.
- Only official email addresses should be used to contact staff or children.
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts.
- All users should be aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail. Notices put in staffroom of new SPAM outbreaks.
- All users should be 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.

- All users should also be aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- Staff are responsible for monitoring the content of children's email communications, both outgoing and incoming messages.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Children are taught how to respond in such situations by reporting immediately to the adult in charge at that time. Staff report to senior leaders within the school and can report to Lancashire directly.
- Users should be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

Social Networks

Social Network sites allow users to be part of a virtual community. They include sites such as Facebook, Twitter, Bebo and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, it may be necessary to access and view other users' content, send messages and leave unmediated comments.

Many Social Network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the teacher through LIGHTSPEED OVERRIDE. Currently, social media sites are not used by school.

All staff need to be aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Any content posted online should not bring the school into disrepute or lead to valid parental complaints. It should not be deemed as derogatory towards the school and/or its employees or towards pupils and/or parents and carers. It should not bring into question the appropriateness of staff to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents,

past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.

- Children must not be added as 'friends' on any Social Network site. School's advice to parents in relation to their use of Social Networking Sites and how the school will respond to identified issues is to refrain from posting inappropriate comments about staff or children that could be construed as instances of cyber bullying. Parents are also requested to refrain from posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Instant Messaging or VOIP

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher

(See <http://www.lancsngfl.ac.uk/lgfladvice/index.php> for more details).

- Staff and children need to be aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.
- Staff do not use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad?
- Only secure messaging, forum or chat systems, e.g. within Moodle, are used.
- Any communication, e.g. Text messaging to contact parents, is to be kept secure and contact lists are stored securely in the school office.

Websites and other online publications

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website.

More details regarding these requirements can be found on the DfE website or at

<http://www.legislation.gov.uk/uksi/2012/1124/made>

- The school website is used as one method to communicate Online Safety messages to parents/carers via links to Online Safety sites and access to the Online Safety policy.
- Everybody in the school who is involved in editing and contributing to the website is made aware of the guidance for the use of digital media.
- Everybody in the school should also be aware of the guidance regarding the inclusion of personal information on the website.

- Editing online publications is restricted to staff who have the responsibility to ensure that the content is relevant and current.
- Overall responsibility for what appears on the website lies with the headteacher in conjunction with the ICT Co-ordinators.
- Consideration is given to the use of any content subject to copyright/personal intellectual property restrictions.
- YouTube is used for teaching if the page has already been checked beforehand.
- Pupils are not allowed to use YouTube themselves.
- Pupils are not allowed to use Facebook
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Infrastructure and technology

School ensures that the infrastructure/network is as safe and secure as possible. School subscribes to the BT Broadband Service and so internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription and is installed on school technology.

Further information can be found at

<http://www.lancsngfl.ac.uk/onlinesafety/>

Children's access

- Children are always supervised when accessing school equipment and online materials (e.g. working with a trusted adult). Use of the computers at break and during lunchtimes is prohibited unless in a supervised club.
- Children's access to the school systems by class logins, Individual logins and age appropriate passwords.
- Children's access is restricted to certain areas of the network and computer.

Adult access

- Access to school systems is restricted for all staff according to their areas of responsibility.

Passwords

- All staff should be aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at <http://www.lancsngfl.ac.uk/online-safety/> website.
- All adult users of the school network have a secure username and password.
- The administrator password for the school network are only available to 'Rustons' as our ICT support provider.
- Staff and children are reminded of the importance of keeping passwords secure.
- Passwords can be changed at the individual's discretion by consultation with the ICT Co-ordinator or the ICT Manager.
- There is agreed format for creating passwords for adults e.g. mixture of letters, numbers and symbols.
- Passwords for classes follow name and number
- Passwords for children are made up by the children and they are taught to keep them secret.

Software/hardware

- School has legal ownership of all software (including apps on tablet devices).
- Rustons keeps an up to date record of appropriate licenses for all software. This is maintained by the ICT Manager.

Managing the network and technical support

- Any servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have been security enabled.
- All wireless devices are accessible only through a secure password.
- Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases.
- ICT technicians are responsible for managing the security of your school network. Monitored by LCC.
- School systems are kept up to date regularly in terms of security e.g. computers are regularly updated with critical software updates/patches and Sophos antivirus software is automatically updated.
- Users (staff, children, guests) have clearly defined access rights to the school network e.g. They have a username and password and, where appropriate, permissions are assigned.
- Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended.
- Users are not allowed to download executable files or install software. The ICT Co-ordinator and ICT Manager possess administrator rights and are responsible for assessing and installing new software.

- Users can report any suspicion or evidence of a breach of security to the ICT Co-ordinator, ICT technician or the headteacher.
- School equipment, such as teachers laptops or cameras, should not be used for personal/family use.
- Any network monitoring takes place in accordance with the Data Protection Act (1998). Staff are told that the network may be monitored from time to time.
- The ICT Manager has been provided with a copy of this policy and is aware of the standards required to maintain Online Safety in the school.

Filtering and virus protection

- Lightspeed Filtering and has requested devolved control over Lightspeed Filtering service.
- **Prevent Duty**, Light speed is complying with the Government's current Prevent Duty guidance.
- (See <https://education.btlancashire.co.uk/annual-services/education-bundle/internet-filtering.aspx> for more details.)
- The filtering is managed by the ICT technician.
- SLT members have access to information regarding devolved filtering in school.
- Information regarding devolved filtering is communicated to members of staff through staff meetings and via email. Staff wishing to block or unblock websites may do so by making a request to the ICT technician or ICT Co-ordinator.
- The ICT technician ensures that all equipment, such as school laptops, used at home are regularly updated with the most recent version of virus protection used in school
- Staff report any suspected or actual computer virus infection to the ICT Technician or ICT Co-ordinator.

Dealing with incidents

An incident log (see Appendix 11) is completed to record and monitor offences. This is audited on a regular basis by Mr Hollinshead (KS2 Leader). Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who must refer this to external authorities, e.g. Police, CEOP or the 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.

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

See chart APPENDIX 12 – Responding to Online Safety Incident Escalation Procedures

Inappropriate use

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Incident Procedure and Sanctions

APPENDIX 12 – Responding to Online Safety Incident Escalation Procedures. In the event of accidental access to inappropriate materials;

- Minimise the webpage/turn the monitor off. Tell a trusted adult.
- Inform Mr Hollinshead who will enter the details in the Incident Log and report to Mr Proctor.

If other people's logins and passwords are used maliciously, inappropriate materials are searched for deliberately, inappropriate electronic files are brought from home or chat forums are used in an inappropriate manner;

- Inform the designated Online Safety Co-ordinator Mr Hollinshead or Miss Martin
- Enter the details in the Incident Log.
- Implement additional Online Safety training with the individual child or class.
- Take appropriate action in relation to the disciplinary policy, e.g. contact parents.

Acceptable Use Policy (AUP)

The Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

The AUP is provided for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. The parental agreement is a partnership between parents/carers, children 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 will be kept in school and made available to all staff.

The AUP reflects the content of the school's wider Online Safety Policy and is regularly reviewed and updated. It is regularly communicated to all users and is understood by each individual user and relevant to their setting and role/ responsibilities.

(see Appendix 4)

Education and training

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 need particular consideration are;

Content

Children need to be taught that not all content is appropriate or from a reliable source.

Examples of risk include;

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

Children need to be taught that contact may be made when using digital technologies and that appropriate conduct is necessary when engaging with these technologies. Examples of risk include:

- Grooming
- Cyberbullying in all forms

- Identify theft (including 'fraud' – 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 or others.

Examples of risk include:

- 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- Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' e-safety. Barden provides relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Regular, planned Online Safety teaching takes place within a range of curriculum areas (including use of the Lancashire ICT Progression document).
- Online Safety education is progressive throughout the school. Staff are provided with a list of suitable sites, resources and activities for their year groups. This list is updated annually.
- Teachers consider how Online Safety education can be differentiated for children with special educational needs.
- St John with St Augustine takes part in the annual 'Safer Internet Day' activities that focus on Online Safety during the National Online Safety Awareness Week.
- During lessons where the internet is used children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications.
- As part of the Online Safety training children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. talking to a trusted adult in school or parent/carer.
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- As part of their Online Safety training and JIGSAW children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.

- Children are reminded of safe Internet use through corridor and classroom displays and the Online Safety rules that are displayed throughout school in infant and junior classrooms.

Online Safety– Raising staff awareness

- Online Safety is regularly discussed at staff meetings and during Inset time.
- Courses are available from Lancashire to train staff with overall responsibility for e-safety, e.g the ICT Co-ordinator and Online Safety co-ordinator.
- Online Safety training/discussions ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- The Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed regularly in staff meetings.

Online Safety– 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).

The school offers opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies both at home and at school through:

- School newsletters, School Website & electronic notice board
- Promotion of external Online Safety resources/online materials

Online Safety– Raising Governors’ awareness

Governors, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date through discussion at Governor meetings, head teachers report, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

NB: The Online Safety Policy is reviewed and approved by the governing body.

Evaluating the impact of the Online Safety Policy

There is a need to monitor and evaluate the impact of safeguarding procedures throughout the school. The headteacher and SLT are responsible for the monitoring and evaluation of safeguarding (including online safety) within St John with St Augustine Primary School. Individual staff are responsible for the recording and reporting of incidents

When monitoring takes place the school should consider:

- Is the Online Safety Policy is having the desired effect?
- Are Online Safety incidents monitored, recorded and reviewed effectively?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the Online Safety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children and how can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of Online Safety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, children and governors informed of changes to policy and practice?
- How often are the AUPs reviewed and do they include reference to current trends and new technologies?