Star of the Sea Catholic Primary School

Online Safety Policy

2024 – 2025

Updated: September, 2024

To be reviewed: September, 2025

Our Online Safety Policy has been written by Star of the Sea Catholic Primary School, building on the Kent and North Tyneside Online Safety draft policies and government guidance. It has been agreed by senior management and approved by governors.

Contents

Policy Aims

- The purpose of Star of the Sea online safety policy is to:
    - Safeguard and protect all members of the Star of the Sea community online;
    - Identify approaches to educate and raise awareness of online safety throughout the community;
    - Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practices when using technology;
    - Enable learners to be empowered to build resilience and to develop strategies to manage and respond to risk online;
    - Identify clear procedures to use when responding to online safety concerns.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, Out of School club staff, agency staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as learners, parents and carers;

- Star of the Sea Catholic Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - Content: being exposed to illegal, inappropriate or harmful material,
    - Contact: being subjected to harmful online interaction with other users,
    - Conduct: personal online behaviour that increases the likelihood of, or causes harm.
    - Commerce: understanding that money can be made from content or 'free' content can be paid for in exchange for data, online gambling, phishing and financial scams and other possible abuses. This could also be referred to as 'transactional'.

Links with other policies and practices

This policy links with several other policies and practices:

- Anti-bullying policy;
- Acceptable Use Policy / Agreement (AUP/AUA)
- Staff Code of conduct / Staff Behaviour Policy / Staff Handbook / Induction procedures
- Low level concerns policy
- OSC brochure
- Behaviour, relationships and discipline policies;
- Child protection policy and Safeguarding Policy;
- Confidentiality policy;
- Curriculum policies, such as: Computing, Personal Social and Health Economic education (PSHE) and Relationships and Sex Education (RSE);
- Data Protection;
- Image use documents;
- GDPR / Information Governance procedures policy.
- Whistle blowing policy

Roles and Responsibilities

Mrs K DiMambro (Head teacher and DSL), Mr L Hall, Mrs L Chidlow and Mr D Thompson (DDSLs) are the online safety coordinators.

Our online safety coordinator's responsibilities are to ensure:

- they keep up to date with online safety issues and guidance through liaison with the Local Authority, and through organisations including The Child Exploitation and Online Protection command (CEOP), NSPCC among others;
- the senior leadership and Governors are updated in line with current Government Guidelines;
- that the policy is implemented and that compliance with the policy is actively monitored;
- all staff are aware of reporting procedures and requirements should an online safety incident occur;

- online safety incidents reported in CPOMs is appropriately maintained and regularly reviewed;
- providing or arranging online safety advice / training for staff, parents & carers and governors;
- natural cross curricular links are made with other taught subjects Computing, RSE, PSHE, RE and others where relevant.

Paragraph 145 in Keeping Children Safe in Education states

> *Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website or LGfL online safety audit.*

Our governors need to have an overview of online safety issues and strategies. Governors are aware of local and national guidance regarding online safety and are updated at least annually on policy developments.

It is acknowledged that all staff have a responsibility to ensure safe practices are modelled onsite in line with guidance in KCSiE. All teachers are responsible for promoting and supporting safe behaviours while in their classrooms, when using technology, and by following school online safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, harassment, abuse or inappropriate materials.

All staff should be familiar with the school's policy.

All staff and visiting adults with access to the school's Internet should sign the Acceptable Use Policy.

Staff are updated about online safety matters at least annually.

Teaching and learning

Why the Internet and digital communications are 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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The Technologies

New technologies are enhancing communication and the sharing of information and are constantly evolving. Current and emerging technologies used in school include:

- e-mail;
- Voice over IP (VOIP);
- Instant messaging, often using simple web cams;
- Blogs (an on-line interactive diary);
- Podcasting (radio / audio broadcasts downloaded to computer or MP3 / 4 player);
- Video conferencing;
- Remote learning platforms;
- Video broadcasting sites;
- Music download sites;
- Devices with camera and video functionality;
- eReaders;
- Other technologies may be introduced throughout the academic year where appropriate.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- the continuation of school provision through remote learning in extreme circumstances through a blended learning approach;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DFE;

- access to learning wherever and whenever is convenient.

Internet use will enhance learning:

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils;
- Pupils will be taught what Internet use is and what is not acceptable and given clear objectives for Internet use;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Pupils will be shown how to publish responsibly and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught the importance of cross-checking information before accepting its accuracy.
Pupils will be taught how to report unpleasant Internet content in school and at home or online e.g. using the CEOP Report Abuse icon.

Blended Learning

In such cases where students are unable to be taught in the school setting Showbie and Purple Mash will be used to continue school provision through a blended learning/remote learning approach.

Remote Lessons (Description of Showbie)

If remote learning is required, Star of the Sea Catholic Primary School will in the main use Showbie to deliver this. Further information on Showbie can be found at https://www.showbie.com

We have planned our remote lesson provision to consider the following

- home access to technology

- children's ability to use the platforms independently
- technical security of the video call
- adult home supervision - (to protect both children and teachers from potential allegations)
    - we advise that camera enabled devices are used in shared family spaces
- the environment of both the children and teachers -appropriate, neutral spaces, e.g. not presenting from or into bedroom spaces
- a second member of staff is present
- if the meeting is recorded or not recorded (with the permission of all involved)
- parent / student acceptable use policies
- age appropriate apps
- parental engagement

Infrastructure and technology

Network Passwords

All users of the school network have a secure username and password.
All staff and pupils are reminded of the importance of keeping passwords secure. If a pupil or member of staff believes that someone other than themselves has become aware of their password, they are to report to their teacher or the online safety coordinator or ICT Co-ordinator and their password will be changed.

Pupil Internet Access

Pupils are informed of available, appropriate materials to use and are supervised by a member of staff when accessing school equipment and online materials, at all times.
Pupils understand that their Internet use is monitored and can be traced to individual users.

Software / hardware

All software and apps have been purchased by the school and is the legal owner.
The dates of appropriate licences are recorded and kept with the secure passwords in the school office.

- The school technician loads any new software onto the school's network.
- The school maintains the licences and arranges to have any software removed when licensing has expired. (School office)

School laptops and iPads are for school work only but can be used off site for work purposes.

Web filtering and virus protection

Virus protection is purchased for the network and all school computers. Regular scans should be performed by staff on devices that are not connected to the Network.

Any device suspected or found to contain any virus or malware must be immediately turned off and removed from the network. The ICT coordinator must then be informed so appropriate technical support can be sought.

(Smoothwall has sophisticated text, image and URL scanning for users accessing and attempting to access inappropriate content. Filtered content is classified by the following categories:

- abuse,
- adult content,
- bullying,
- criminal activity,
- radicalisation,
- substance abuse,
- suicide.

All breaches are logged by Smoothwall and can be traced back to identify school, machine, time and date. Logs of misuse can be obtained from the LA on request.

While strong filters are in place, no filtering is 100% effective and so staff must remain vigilant for inappropriate content when using the Internet. If anything inappropriate is found, staff should turn off the screen of the machine and remove it from use. They should then (when it is safe to do so) screen capture the website and report it to the online safety Coordinators and also ict.helpdesk@northtyneside.gov.uk so it can be reviewed, blocked and reported if necessary.

Staff may also request for websites to be unblocked if they believe they are appropriate for educational purposes by contacting the LA corporate ICT helpdesk at ict.helpdesk@northtyneside.gov.uk

Staff are permitted to use an amended version of the primary filters that allow access to Youtube and Facebook via a proxy. This has been agreed by senior management in school but must only be used on staff devices. Staff must still exercise caution when using sites like Youtube and pre-plan videos to be shown and avoid 'live searches' for videos in class where possible. Sites such as 'quietube' can be used to show just a video without comments and related videos etc. in class, this can reduce the risk of students being exposed to unsavoury comments below a video.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
School ICT systems security will be reviewed regularly and security strategies will be discussed with the Local Authority.
Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation (IWF) or CEOP: Child Exploitation and Online Protection command.

Managing the network and technical support

The server and cabling is securely located and its physical access is restricted. The network is managed by St Thomas More Academy.
The internet delivery is monitored via the council.

Requests for technical support can be made via a ticket log or to primarysupport@stmacademy.org.uk

Use of Technology

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Devices including phones and smart watches

Students can bring personal devices to school, school accepts no liability for the device and it must remain unseen throughout the day.

Staff use

Our school allows personal mobile phones to be used in school by staff and visitors, however they are not to be used within the classroom or when pupils are present. Phones should be turned off or on silent during lessons.

Digital Communication

Email – Our email solution is purchased through the Local Authority as part of the ICT SLA using NTLP Google.

Staff and pupils may only use approved email accounts on the school system.

All NTLP Gmail is filtered. Email content, titles, addresses and attachments are scanned for questionable content, which is maintained by LA admin staff. Mail that breaches the guidelines for security or appropriateness is blocked from reaching its intended destination and placed into a quarantine folder. Quarantine items are checked by LA staff on a regular basis and reports are made to Headteachers where anything of concern is captured.

All pupils on roll automatically get an account created as they are added to our schools SIMS database. However, students are only provided with their login details during the term when email is taught.

NTLP Password policy for staff is as follows:
Your password must be at least 8 characters in length. It must contain both letters and numbers. The following symbols are allowed but not required: !'"£$%^&()+_=-:@~][?.,/*

Student NTLP passwords must be at least 6 characters for primary aged pupils. There is no requirement to change them on any timescale.

- Pupils must immediately tell a teacher if they receive offensive email;
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone;

- Incoming email should be treated as suspicious and attachments not opened unless the sender is known;
- E-mail sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The sending of abusive or inappropriate email messages is forbidden;
- Electronic mail should only be used in the course of work as a student and only using the authorised logins provided by the school;
- Users must never use electronic mail to send or forward chain letters or any material which may contravene school policies (e.g. jokes, pictures of a racist, homophobic or sexist nature);
- Users must only copy messages (i.e. cc or bcc) to people where it is of direct relevance.

Staff use

- Staff are expected to check their email mailboxes regularly, at least twice a day.
- The use of personal web based email in school is forbidden to minimise the risk of unsuitable materials and viruses from external email accounts.
- All users are aware that email is covered by GDPR, meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails, this is provided by the Local Authority and is standard in all emails sent via NTLP.

- Staff are required to add a standardised email signature covering Name, Role in school and contact details.

Social Networks for school communications

School communication

- The school will control access to social networking sites (Twitter) for school communication;
- Newsgroups will be blocked unless a specific use is approved;
- Pupils and parents & carers will be advised that the use of social network spaces outside school brings a range of dangers for pupils and app age limits should be taken into account;
- Permissions will be sought before any content relating to a child is posted on a social media site. This is done on an annual basis via consent form which is available on the school website.

School does not encourage any social media accounts set up in the school's name by any parents or carers.

In line with this policy:

- Staff are expected to manage their digital identity and portray themselves in a positive, professional and appropriate manner when posting or sharing content online;
- Staff should have privacy settings in place and should check and review these on a regular basis;
- Staff should not give personal contact details to pupils or parents & carers including mobile telephone numbers, details of any personal blogs or websites;
- Staff should not add pupils (past or present) as "Friends" on any Social Network site;
- Staff should never post on behalf of, or refer to the school, pupils or parents & carers on any social networking site, unless it is from the school's official accounts and with the permission of the Headteacher teacher;
- Users of social media should consider copyright of the content they are

sharing and, where necessary, should seek permission from the copyright holder before sharing;
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Instant Messaging:

Instant Messaging, e.g. Whatsapp, Facebook Messenger etc. provide an opportunity to communicate in real time using text, sound and video. It is not appropriate to use these tools in school.

G suite and Showbie provide their own filtered instant messaging 'chat' and 'video chat' services, which should be the only messaging service used in school, and then only used by students with adult permission for remote or blended learning.

Published content and the school website

The school website is www.staroftheseaschool.co.uk It provides key information to the public about the school, promotes the school and celebrates pupils' work.

Staff or pupil personal contact information will not be published.

All teaching members of staff have administrative rights to edit our school website: The Headteacher will take overall editorial responsibility and will ensure that content is accurate and appropriate.

Our website is fully compliant with Government and Ofsted requirements for schools maintained by a local authority.

Video conferencing

Video conferencing is available through Showbie, G suite (Meet)and Microsoft 365 (Teams), using the video chat facility when a webcam is available.

Use of video conferencing / video chats may be deemed necessary to enable some aspects of remote learning to take place. Any use of external video conferencing software must not be done with a teacher's 'personal' account. An adult must always be present in the room when any video conferences / chats are taking place. The regulations for using webcams are similar to those for CCTV. This means that the area in which you are using the webcam must be well signposted and people must

know the webcam is there before they enter the area, in order to consent to being viewed in this way. Children should be consulted and adults would need to consent as well as the parents & carers of all children involved.

In gaining consent, you must tell the person why the webcam is there, what you will use the images for, who might want to look at the images and what security measures are in place to protect access.

As children also have access to NTLP Google Meet video chat outside of school, they must also be educated about safe, appropriate and acceptable use of these technologies, considering the following points:

- how, when and why they make use of it;
- ensuring an appropriate adult knows they are using it;
- never accepting a chat request from someone they do not know;
- reporting anything they find upsetting or inappropriate in a video chat to a trusted adult;
- protecting their personal information when using it. This may include not just what they say in a 'chat', but even the objects in the room around them which may inadvertently give away personal information they don't wish to share.

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school are required to follow the school's guidance below.

- All staff and pupils are instructed that full names and personal details should not be used on any digital media, particularly in association with photographs;
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children are preferable;
- We ask all parents & carers to provide written permission stating whether or not they can have their photograph taken and used within school or on the school website;
- Pupil image file names will not refer to the pupil by name;

- All staff are instructed of the risks associated with publishing images, particularly in relation to use of personal Social Network sites;
- Our school ensures that photographs / videos are only taken using school equipment and only for school purposes;
- We do not allow staff to store digital content on personal equipment;
- When taking photographs / video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted;
- Staff, parents & carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved. They are made aware of these dangers through online safety lessons and training from outside agencies;
- Parents & carers are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories;
- Staff sign an AUP informing them of the guidelines for safe practice relating to the use of digital media, as outlined in the schools' policy. These are monitored by our online safety coordinator and SLT.

Protecting personal data

Personal data will be recorded, processed, transferred and made available in line with GDPR.

Policy Decisions

Authorising Internet access

- All staff and visiting adults who use the school Internet or technology must read and sign the Acceptable Use Policy before using any school ICT resources;
- All pupils must read and sign the Acceptable Use Policy before using any school ICT resources;
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- The parent / carers of N-Y1 children will be asked to sign a parents & carers or Family AUP before school email account details are shared to support remote learning.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials;
- At Key Stage 2, pupils accessing the Internet are directly supervised by a member of staff;
- Extended school provision accessing the Internet are directly supervised by staff on directed sites.

- parents & carers will be given details of the acceptable use agreement that pupils have signed;
- This online safety policy will be published on the school website and advice on the safe use of the Internet will be provided.

Handling online safety incidents

Our online safety coordinator acts as the first point of contact for any complaint. The Local Authority supplies the following document to suggest appropriate action when dealing with online safety, and in particular social networking related, incidents. [Click here to access - How to deal with an online safety incident involving staff 2019 v3]

Assessing risks

The school will take all reasonable precautions to ensure online safety and prevent access to inappropriate material. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school site.

- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate and effective;
- Methods to identify, assess and minimise risks will be reviewed regularly;
- The SLT will ensure that the online safety policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Incidents involving pupils

- Incidents of cyberbullying are dealt with in accordance with our bullying and behaviour policy;
- Incidents related to child protection are dealt with in accordance with the school's safeguarding and child protection policy and reported to the Headteacher immediately.
- If an incident occurs involving a pupil misusing the Internet / equipment, the member of staff in charge should seek the nearest member of staff to witness the misuse, protecting them against any incident / allegation towards themselves.
- The device where the incident took place (if in school) must be taken out of use until appropriate evidence can be captured to log the incident;
- All staff are made aware of different types of online safety incidents and know that they must report them immediately.
- Once incidents have been reported, a record must be made by the member of staff involved, which will then be filed on CPOMS.
- If necessary the Local Authority will be informed of any misuse and parents & carers will be informed.
- Pupils and parents & carers will be informed of consequences for pupils misusing the Internet.
- Parents & carers and pupils will need to work in partnership with staff to resolve issues.

As with other safeguarding issues, there may be occasions when other outside agencies must be contacted. Incidents of a criminal nature; i.e. threatening, intimidation or harassment may then involve contact with the police for further advice (at the discretion of the Headteacher).

Parents & carers and pupils are given information about infringements and possible

sanctions. Sanctions for pupils include:

- informing parents or carers;
- removal of Internet or computer access for a period of time.
- referral to LA / Police.

Incidents involving staff

- Any incident involving staff misuse must be referred immediately to the Headteacher.

If a member of staff suspects that they are in breach of this policy whilst acting in good faith they must notify the Headteacher or nominated online safety coordinator IMMEDIATELY so that action can be taken to prevent or minimise damage.

Any authorised user who commits a breach of any school policy as a result of unauthorised use of electronic media may face disciplinary procedures. If the school discovers that a member of staff has committed a criminal offence or has been a party to the commission of one as a result of unauthorised use of electronic media the police will be contacted immediately. The school will in no way indemnify a member of staff who has incurred any liability as a result of unauthorised use of electronic media. The school will seek financial redress from an authorised user whose misuse of electronic media causes the school to suffer a loss.

Incidents involving other adults (e.g. parents & carers)

- Any incident affecting the school but involving other adults out of school must be referred immediately to the Headteacher;
- Where possible, evidence should be collected immediately and individuals concerned may be contacted by the Headteacher to discuss the incident;
- If necessary the Local Authority will be informed of any misuse;
- Incidents of a criminal nature; i.e. threatening, intimidation or harassment then may involve the police for further advice (at the discretion of the Headteacher).

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly;

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up;
- A programme of training in online safety will be used with staff and students.

Online safety training will be embedded within the computing scheme of work and the Personal Social Health Economic (PSHE) curriculum. Key resources to support this are Project Evolve from South West Grid for Learning and the UK Safer Internet Centre, and Common Sense Education's Digital Citizenship curriculum.

Staff and the online safety policy

- All staff will be given the online safety policy and its importance explained;
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and follow clear procedures for reporting issues;
- Staff will always use a safe search engine when accessing the web with pupils;
- The school will liaise with the LA as part of the ICT SLA to provide effective support to staff.

Enlisting parents' and carers' support

- Parents and carers will be reminded of the acceptable use policy for children at the start of each academic year;
- Throughout the year parents and carers will be reminded about the online safety policy in newsletters, the school brochure and the school website;
- Star of the Sea Catholic Primary School will maintain a list of online safety resources for parents & carers;
- The school will liaise with the LA as part of the ICT SLA to provide effective support to parents and carers.

Standards and inspection

- Staff will regularly remind children of online safety rules and any incidents that occur will be reported to the online safety coordinator;
- Each incident that takes place will be reviewed by the online safety

coordinator and appropriate action will be taken immediately;
- Incidents will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, individual children etc.;
- If a pattern emerges they will be addressed through targeted interventions with the appropriate groups;
- All stakeholders are informed of changes to policy and practice via newsletters, meetings and training sessions;
- AUPs are reviewed annually and updated to include new technologies, when necessary.

Prevent Duty

As of 1 July 2015, all schools, and registered early years and childcare providers are subject to section 26 of the Counter-Terrorism and Security Act 2015, also known as the Prevent duty. This states that they must have 'due regard to the need to prevent people from being drawn into terrorism'. Issues relating to this are covered in the school safeguarding policies, but the school is also aware of the risks that digital technologies pose for young people in being exposed to radicalisation and extremism. Much of this policy covers the ways in which school strives to keep young people safe and minimise risks they face while they engage with technology.

Leavers Policy

What to Do When a Teacher / Staff member Leaves

The purpose of this section is to:

- Help ensure that school's data and resources remain secure as personnel leave the organisation
- Help reduce the opportunity for misplaced or malicious allegations.

Adults who work in schools may have access to a range of important and sensitive information including images and personal details of colleagues and learners and it is essential that the integrity of the school's systems and files remain intact when colleagues leave the school.

Email – disable password. School technical administrators may need to keep access to the account by forwarding mail to an alternative account. This will help address any ongoing issues, projects that need to be completed, outstanding actions etc.

Network – change access password. Delete files or inspect prior to making them available to other users.

Secure areas – ensure key codes are changed and all keys retrieved.

Portable devices – need to be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.

Learning platform – account disabled but not deleted. This will ensure all useful documents can continue to be used by the school. Ownership of necessary documents should be altered as soon as is practicable.

Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.

Images – no teacher can take images of pupils away from school when they cease to be employed by the school.

What to Do When a Pupil Leaves

Network – remove log-in from system. Delete files or inspect prior to making them available to other users.

Learning platform – accounts are linked to the SIMS database, as pupils are removed from SIMS they are removed from the school. If they move onto a new school the accounts will be transferred. When they leave the North Tyneside school system their account will be suspended.

Staff, Governor and Visitor - Acceptable Use Agreement / Policy (AUP)

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This AUP is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarifications should be discussed with the Headteacher.

Content:

- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent / carer, member of staff or Headteacher.

Contact:

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

Conduct:

- I understand that ICT includes a wide range of systems including devices, email, social networking and that ICT use may also include personal ICT devices when used for school business. I will use them responsibly and inline with the relevant policies.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will not give out my own personal details, such as mobile phone numbers and personal email address, to pupils / parents / carers.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any member of the school community
- 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, offensive, illegal or discriminatory comments made on social network sites, forums and chat rooms.
- 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.
- I will not use the school system(s) for personal use during working hours.
- 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.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- 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 and potentially illegal.
- I acknowledge that when I am logged on to a school computer, I am responsible for its overall use, including use of the Internet.

Commerce:

- I will respect copyright and intellectual property rights.
- I will always consult the Headteacher before ordering any goods intended for school use via the Internet.

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.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name ..... Job title.....

Star of the Sea Catholic Primary School

Pupil - Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to make sure that there is no risk to myself, the school or others.
I understand that everyone has equal rights to use technology as a resource.
I will act as I expect others to act toward me.
I recognise that the school has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of Star of the Sea Catholic Primary School.
I understand that I am responsible for my actions, both in and out of school.

Content:

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will not try to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work;

- I will not use Star of the Sea Catholic Primary School systems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- I will respect others' work and will not access, copy, modify, or remove any other user's files without permission.
- I will not take, store or share images of anyone without their permission;
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others;
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Contact:

- I understand that some people pretend to people they are not online;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language;
-

Conduct:

- I understand that Star of the Sea Catholic Primary School will monitor my use of the systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, or try to use anyone else's accounts;
- I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will not share personal information about myself or others when on-line (e.g. names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.);
- I understand that Star of the Sea Catholic Primary School systems and devices are intended for educational use and that I will not use them for personal use unless I have permission;

- I will not open any hyperlinks or attachments in emails, unless I know and trust the person who sent the email, or if I have any concerns about the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings;
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings;
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;

Commerce:

- I will immediately report any damage or faults involving equipment or software, however this may have happened;
- I should ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not try to download copies (including music and videos);

I understand that if my actions in or out of school go against any of the statements in this document Star of the Sea Catholic Primary School can impose school sanctions.

Student Signature

I agree to follow the rules and to support the safe use of ICT throughout the school

Full Name ……. Date ……

Parents / Carers Name ……. Date ……

Additional Useful Documents

- Keeping children safe in education
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Searching, screening and confiscation at school
- Challenging victim blaming language and behaviours when dealing with the online experiences of children and young people
- Harmful Harmful online challenges and online hoaxes
- The Prevent duty
- Prevent duty training
- What maintained schools must publish online
- Safe remote learning - SWGfL
- Safer blended learning advice from UK safer Internet Centre
- NSPCC Consultancy Team
- Safeguarding and child protection self-assessment tool
- national.lgfl.net/digisafe/onlinesafetyaudit