March 2017

E-Safety Policy & Practice 2017-18

Whole School

Contains relevant information on safety measures for pupils and staff when accessing and using the Internet, storage, data protection and breakdown/disaster.

Stanley School e-Safety Policy

The Acceptable Use of the Internet and Related Technologies – Code of Conduct

Updated January 2017
Date for Review January 2018

Our E-Safety policy relates to other policies including those for ICT, bullying and for child protection/safeguarding.

The School's E-Safety Coordinator is the Head Teacher (Anthony Roberts)

Our E-Safety policy has been written by the School, building on the Wirral E-Safety Policy, whilst reviewing guidance from BECTA (no longer a government agency) and the Department for Education.

It has been agreed by senior management and approved by governors.

The E-Safety Policy was revised by Jon Lenton, Wirral ICT Advisory Teacher.

Introduction to E-Safety

1.1 E-Safety in a changing world

The term E-Safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At Stanley School we celebrate the value and importance of technology in our children's learning. In our school, personal computers, wireless laptops, I-pads, camcorders and digital cameras are all part of children's every day learning. The Internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies such as Ipads and the Internet on a daily basis and experience a wide range of opportunities and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education; for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety policy;
- A well thought out approach regarding how to develop E-Safety guidance within the school's curriculum.
- Identify opportunities to ensure that we support families with the challenges relating to E-Safety in the digital age (family workshops, web-links, etc.)
- Secure, filtered broadband from Wirral Council's Network;
- A school network that complies with the National Education Network standards and specifications.

1.2 e-Safety and the legal issues

E-Safety should be applied to protect children, staff and all members of our school community. Our School's e-Safety policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications, such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example, it is a criminal offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children. In addition, there are many grey areas for schools to consider regarding communication of social network sites, storage of data, etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that:

- It has effective firewalls and filters on our school network.
- Ensures that e-Safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors
- Ensure that our procedures are consistent with the Data Protection Act (1998)

Learning and teaching in the digital age

The School uses wireless laptops and Ipads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of the School's curriculum. However, the school will include provision to educate children on how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile communication equipment and the Internet are 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. We also recognise that children are actively engaged with digital communication from an early age. It is part of their lifelong learning experiences and habits. This generation are what Marc Prensky refers to as, 'digital natives'. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition, use of the Internet is part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through Local Authority provision and the School's network arrangements with RM. Only sites approved by the Head Teacher will be allowed to override the filter.

- Pupils will be taught about responsible and appropriate information sharing through the Internet and other forms of digital communication.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.

- Pupils will be educated in the effective us of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication 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 or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

2.4 Our School will support all pupils by:

- Ensuring the content of the curriculum includes social and emotional aspects of learning; Through PSHE and other curriculum contexts, pupils are encouraged to talk about feelings and deal assertively with pressures, are listened to, and know to whom they can turn to for help and advice;

- Ensuring a comprehensive curriculum response to e-safety, enabling children and parents to learn about the risks of new technologies and social media and to use these responsibly;

- Ensuring that the curriculum will help children stay safe, recognise when they do not feel safe and identify who they might or can talk to;

- Ensuring the school curriculum will support young people to become more resilient to inappropriate behaviours towards them, risk taking behaviours and behaviours that children may be coerced into including 'sexting';

- Sexting – children in Year 5 and 6 (where appropriate) will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.

- Providing pupils with a number of appropriate adults to approach if they are in difficulties;

- Supporting the child's development in ways that will foster security, confidence and independence;

- Encouraging development of self-esteem and self-assertiveness while not condoning aggression or bullying; (Our Anti-bullying policy can be found in the School's behaviour policy on the School's website).

- Ensuring repeated hate incidents, e.g. racist, homophobic, radicalisation or gender- or disability-based bullying, are considered under safeguarding procedures;

- Liaising and working together with other support services and those agencies involved in safeguarding children;

- Monitoring children who have been identified as having welfare or protection concerns and providing appropriate support.

- The School behaviour policy is aimed at supporting vulnerable pupils in the School. The School will ensure that the pupil knows that some behaviour is unacceptable but that they are valued and not to be blamed for any abuse which has occurred.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is a vital element of promoting e-Safety.

The school will ensure that permission for access and use of any content, including photographs and video is fully explained and sought on admission to the school.

3.1 Information system security

- School ICT systems security will be reviewed regularly. This will be part of the liaison between the Head Teacher and the Wirral's Technical Services department.

- Virus protection will be updated regularly as part of the school's Service Level Agreement with the Local Authority.

- Security strategies will be discussed with the Local Authority.

3.2 Managing filtering

- The school will work with Wirral Local Authority and other national bodies to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator, Louise Wharton.

- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3 E-mail

- Pupils may only use their school approved e-mail account (e-Schools) on the school system. All use of other e-mail accounts is prohibited.

- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the acceptable use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organisations associated with the school.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The forwarding of chain letters is not permitted.

3.4 Published content and the school website

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff.

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 Publishing pupils' images

- Photographs that include pupils will be selected carefully. The school will always risk assess/review photographs for possible abuse.
- Names or any other personal details will never be published alongside photographs.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories, Guidance @ Children, Families, Health and Education Directorate, page 6, June 2008.

3.6 Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate pupils in their safe use. The school will use the Virtual Learning Environment to teach children about social interaction and communication on the Internet. This will be carefully managed. All staff will seek the approval of the Head Teacher before using any sites with children. Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Staff members are fully informed of their responsibilities regarding the use of social networking sites such as Facebook. At Stanley School we have agreed that it is good practice to separate professional and personal commitments. Therefore, the following groups would not be allowed as contacts and friends on social networking sites:
    - Ex pupils or current pupils; the context of teacher to pupil relationship is not suitable for social networking
    - Parents; we believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.
- All staff members are also aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organisations associated with the school.
- Staff members are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility.

NUT cyber-safe guidance states all staff should:

- Not post information and photos about themselves, or School-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see;
- Keep passwords secret and protect access to accounts;
- Not befriend pupils or to other members of the School community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this).

NASUWT guidance states:

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.

- Do not, under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.

As a minimum, NASUWT recommends the following:

Privacy setting	Friends only
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you are tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check into	Friends only
Contact information	Friends only

- Always make sure that you log out of Facebook after using, it, particularly when using a machine that is shared with other colleagues/student. Your account can be hijacked by others if you remain logged in, even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click, "clear chat history", in the chat window).
- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

<u>Conduct on social networking sites</u>

- Do not make disparaging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.

- Act in accordance with your employer's information technology (IT) policy and any specific guidance on the use of social networking sites. If your school/college encourages the positive use of social networking sites as part of the educational process, they should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries.

- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. If you face disciplinary action as a result of being tagged, contact NASUWT immediately.

- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.

- If you have any concerns about information on your social networking site, or if you are the victim of cyber bullying, you should contact your NASUWT Regional Centre immediately.

- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access your bank or credit card account.

- Be aware of what monitoring, if any, may be carried out by the school/college. Full details of this should be detailed in the IT policy.

- Stop the network provider from passing on your details of other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "advertising purposes", for example, to stop Facebook from forwarding your details, click "privacy settings". Under "applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.

- Ensure that any comments and /or images could not be deemed defamatory or in breach of copyright legislation.

POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, e.g. Facebook, Twitter, Bebo and its implications in relation to future employment status, i.e. disciplinary action and potential dismissal. The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years.

Any member of staff can have an account on a social networking website; however, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

Please note: **School employees who have their own social networking site may have contact with relatives or family friends. However, all the requirements below would still apply to the use of Social Networking Websites.**

All school staff **must:**

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking websites.
- Ensure that any content shared on any social networking website, at any time, would be deemed as appropriate, i.e. staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.
- Ensure that any comments and/or images, at any time, could not be deemed as defamatory, or in breach of any relevant legislation.

All school staff **must not:**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role, e.g. music tutor, on any social networking website.
- Use social networking sites as a forum to make a derogatory comment which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority, or the wider community.

Any breaches of this policy could result in disciplinary action and may result in your dismissal.

In signing this policy, you understand and agree to adhere to the policy on the use of social networking websites.

This guidance is applied through the Local Authority's policy on the agreed use of social networking sites and the school's acceptable use and E-Safety code of conduct. All staff and visitors, including students, have to sign these then they join our staff team.

3.7 Managing videoconferencing and webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff. At Stanley School we will only use webcams for specific projects and full consent will be sought before children participate in these. Examples may be conferencing with another school in India.
- All software for webcam use will be password protected (Skype, etc.)
- Best practice recommends that schools always seek consent from parents for any video-conferencing.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. For example, mobile devices are allowed in school for children in years 5 & 6 but these are stored in a secure classroom based locker. Staff are allowed to have mobile devices in school but these must not be used during the working hours except for school or emergency based communication in office areas or the staffroom and PPA room.

- The senior leadership team should note that technologies, such as mobile devices with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Personal mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages, or files by Bluetooth, or any other means, is forbidden.

- The use by pupils of cameras in mobile devices is not allowed.

- Games machines, including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. They can be used in school but NEVER for online gaming or Internet access.

- Staff will be issued with a school mobile phone where contact with pupils is required or school camera to capture photographs of pupils. Staff must not take photographs on their personal phones. Guidance @ Children, Families, Health and Education Directorate, page 7, June 2008.

- The appropriate use of Learning Platforms will be discussed annually.

3.9 Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff members are aware that they have a professional responsibility to ensure the following:

- Personal data will be password protected. Work laptops cannot be used for the storage of any inappropriate material.

- Photographs in DropBox should only be accessed in school and should be moved into the school media storage folder and deleted from the device also.

- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.

- Photographs cannot be stored on personal laptops. The only exceptions are finger-tips e-profile data and the archive stored by the Head Teacher.

- No data or images can be transported out of the school without the device being approved or password protected.

3.10 Use of photographs

The Data Protection Act 1998 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years for any photographs or video recordings for purposes beyond the school's core educational function (e.g. school websites).

3.11 Computing Software – Code of Conduct

The Code of Conduct relates to Wirral's policy concerning software duplication. Unless otherwise provided for in the licence agreement, any duplication of copyrighted software, except for backup and archival purposes, is a violation of the law and is contrary to Stanley School's standards of conduct.

The following points comply with software licencing agreements:

- All computer software used by the School is purchased through the 'Purple Mash' provider. Access to the software is through personal username and password which enables the user to access programmes both at School and at home.

- I-pad software is purchased through the School's I-Tunes account, which is properly regulated by the Apple Corporation. Access is through personal username and password with the appropriate licensing.

- All software is used in accordance with the licence agreements.

- The School does not condone and will not tolerate illegal copying of software or copyright documentation under any circumstances. Anyone who copies, uses or otherwise acquires unauthorised software shall be subject to disciplinary procedures and could also be subject to civil and criminal penalties including fines and imprisonment.

- No employees are given or allowed to loan software to any unauthorised persons including clients, customers and others.

- Any employee who determines that there may be misuse of software within the School shall notify the Head Teacher or their Line Manager.

All software is approved and installed by the Local Authority through our Service Level Agreement.

3.12 Data Security

The Data Protection Act 1998 is designed to protect the rights of individuals in relation to the personal data that is held about them. It sets out requirements about the processing, storage and disclosure of that data and extends the coverage of the previous legislation from data handled electronically to certain manual record systems.

The Act requires governing bodies and head teachers to notify the Data Protection Commissioner where the activities they are engaged in are covered by the legislation. It is highly probably that pupil records will fall wholly or partly under the requirements of the Act and be subject to notification.

Security of Access

Computer systems used for school management are protected by password security to ensure that only authorised staff members have access. The Local Authority advises staff that passwords should be changed regularly every 30 days and ensures passwords are cancelled immediately when staff members leave.

Data protection legislation states that all those who hold persona data, including schools, whether on paper or electronically, must keep that data secure. Personal data is defined as any combination of data items that identify an individual and provides specific information about them, their families or circumstances. This includes their names, contact details, gender, dates of birth, unique pupil number (UPN) as well as other sensitive information such as academic achievements, other skills and abilities, and progress in school. It may also include behaviour and attendance records.

The governing body ensures that the Data Protection Commissioner is notified in accordance with the Data Protection Act 1998 and that the School's use of any electronic or relevant manual systems to record or process personal information, and any disclosure of that information, complies with the legislation.

Stanley School renews its Data Protection Register on an annual basis through the Registrar Data Protection Commissioner.

The following accompanying good practice guides from Becta provide a description of the procedures and possible technical and operation solutions that will assist the School in minimising the risk of data security incidents and complying with existing Local Authority legislation. These good practice guides have been read by senior school staff responsible for implementing technical solutions:

Impact levels and labelling
Data encryption
Audit logging and incident handling
Secure remote access

- Data is classified as either level 2 or 3. All highly sensitive date, including photographs of pupils, is classified at level 2 and is subject to encryption through programmes installed on laptops, computers and tablets.

- All portable computing equipment is transported in lockable carriers and stored on site in lockable cupboards/rooms.

- All remote access is restricted by password access and other protocols engaged when required.

- Disused computing equipment and external drives, including memory sticks, are 'ghosted' by the Local Authority technicians.

- The Local Authority ensures protection against viruses by installing and regularly updating anti-virus software, by blocking he use of unauthorised software, by filtering and blocking unsuitable Internet sites and ensures that information access and downloads are in compliance with their Control Policy and Internet Code of Conduct.

3.13 Computer Disaster Recovery Plan

Administration and curriculum data is automatically backed up by the Local Authority as part of the 'CARS' network system with a remote access for all files located on the School servers. The Local Authority has advised there is no requirement to back up any of the data stored on this system; recovery is through the Local Authority in the event of a breakdown/disaster.

All computing equipment, including tablets are stored in a separate locked store room. Access is by restricted fob.

All equipment is security logged for insurance purposes in the event of a fire.

The School has a fully operational fire and intruder alarm system.

Introduction

E-safety may be described as the school's ability to:

- Protect and educate pupils and staff in their use of technology.
- To have the appropriate mechanisms to intervene and support any incident where appropriate.

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, or causes, harm.

Why is Internet use important?

The purpose of the Internet use in school is to raise educational standards, to student achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element of 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Stanley School has a duty to provide students with quality Internet access.

More able pupils will use the Internet outside school and will need to learn how to evaluate Information and to take care of their own safety and security.

How Can Internet Use Enhance Learning?

- The School's Internet access is designed expressly for student use and includes filtering appropriate to the age of the pupils.

- More able pupils will be taught what Internet use is acceptable and what is not given clear objective for Internet use.

- Internet access will be planned to enrich and extend learning activities.

- Staff will guide students in on-line activities that will support learning outcomes planned for the pupils' age and ability.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- All staff and pupils have access within school to the Internet.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Head Teacher. The E Safety concerns form is located in the school office and must be filled in and returned to the computing coordinator or directly to the head teacher and recorded in the e-Safety log.

- Stanley School will ensure that the use of Internet derived materials by pupils and staff complies with the copyright law.

- Staff and pupils will be aware of the materials they are shown and how to validate information before accepting its accuracy.

E mail

- Pupils will only use approved e-mail accounts on the school system.
- If by any chance a pupil receives an offensive e-mail they must tell the teacher immediately.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Email Benefits

An email account allows staff to facilitate communications with the Local Authority staff and support services, professional associations and colleagues.

Email Use

Staff are allowed to access personal emails with their school account, provided the following conditions are adhered to:

Appropriate Use

- Staff need to be aware that emails are easily forwarded, so be professional and careful about what you write.
- All emails should be regarded in the same way as messages on school headed notepaper.
- The downloading and sending of copyright material is prohibited.
- None of the following should be deliberately sent:
    - Pornographic language
    - Pornographic pictures
    - Information which may be considered offensive or threating to others
    - Defamatory or illegal information

Standards

- Email standards for sending and receiving emails to ensure the effective use of the School email system.
- Emails should only be read by the intended recipient.
- Staff should open their email a minimum of twice per week
- All incoming emails should be replied to within 10 working days, or acknowledged within 5 days. Certain emails may need to be prioritised in light of their content.
- In the case of absence you should set up an auto-responder if possible. This should provide an alternative contact and length of absence if known.
- All staff should regularly organise mail to ensure the mailbox does not exceed 76% full.
- A signature should be added to any email sent. This should include your name, position, and contact details in addition to the disclaimer as stated below:

"This email and any files transmitted with it are confidential and intended solely for the use of the named recipient. If you have received this email in error please notify Stanley School, Wirral, and/or sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the School; finally, the recipient should check this email and any attachments for the presence of viruses. The sender accepts no liability for any damage b any virus transmitted by this email".

Security

- Staff should keep their password confidential and it should not be disclosed under any circumstances.
- Staff should change their password occasionally.
- Staff may only use their own password protected accounts to send and check email.
- Sensitive information should be sent by post or via a secure transfer system.
- Important emails need to be saved securely using a hierarchical file structure.
- Certain emails may need to be printed.
- Staff must not leave their mailbox open and unattended.

Safety

- Only register your email address with reputable organisations.
- Never give personal details out over the Internet, unless you have initiated the transaction and you are confident of the identity of the receiving party.
- Never open, reply or forward span (junk mail).
- Inform Reception if you regularly receive junk mail into your account.
- Staff who receive inappropriate email need to inform IT Services immediately; the email must not be replied to.
- Be cautious when opening attachments; save any attachments to the computer's hard drive to ensure they are scanned before opening.
- Report any problems with your email account to IT Services for resolution.

Monitoring

The purpose for which monitoring is conducted would be explained fully.

- Your response times to email may be checked from time to time to ensure that you are regularly accessing your account.
- The content of emails will only be monitored if there is clear evidence that serious misuse has occurred.
- If banned words are sent an automated email will be sent to you.
- If an email address is sent to a non-existent address (this may occur by typing the email address incorrectly), this will result in a failure message and the contents of your email being returned to the sender.
- If your email contains a virus, your email is not sent and you will receive a copy of the undeliverable email and attachment

Sanctions

- The Head Teacher will be responsible for ensuring that this policy is implemented effectively.
- Deliberate misuse of email will result in disciplinary action taken against you.

Social Networking

- The School will block / filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind which may identify them or their location. This is also taught under Protective Behaviours.
- More able pupils will be taught not to place personal photos on any social network space.
- More able pupils will be advised about security and encouraged to set passwords.
- Pupils will be encouraged to invite known friends only and deny access to others.

Face Book

- This is a great way to communicate with friends and relatives but caution should be taken when it is used in the professional context.
- Staff are aware that 'any' reference to school matters that is accessible to other staff, pupils, parents and members of the public has the potential to cause upset and could lead to disciplinary action against that

person.
- Staff are aware that the school adheres to the Council's policy on Harassment and Intimidation. The definition includes behaviour which may create an intimidating, unwelcoming and stressful work environment or cause personal offence or injury. It also notes that this can consist of a number of trivial incidents. It is not difficult to see how messages posted on Face Book could contribute to this.

Filtering

The school will work in partnership with the Wirral Local Education Authority and Becta to ensure filtering systems are effective as possible.

Video Conferencing

Pupils will always be supervised at all times if ever opportunities arise for video conferencing with others arises.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones / handheld communications devices / gaming consoles will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site

- The contact details on the School's Website will be the school address, e-mail and telephone number. Staff or pupil personal numbers will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Students' Images and Work

- Photographs that include pupils will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the Web site or VLE, particularly in association with photographs.
- Written permission from parents or carers will be obtained as part of the welcome pack when the pupil starts school before photographs are used on the website or VLE.

Information System Security

- School computing systems' capacity and security will be reviewed regularly by the School's computing team and the Local Authority through outsourced Service Level Agreement.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and technicians.

See also Data Security Policy.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the School nor Wirral Metropolitan Council can accept liability for the material accessed, or any consequences of Internet access.

Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher. The E Safety concerns form is located in the school office and must be filled in and returned to the computing coordinator or directly to the head teacher and recorded in the e-Safety log.

Communication of Policy

- All staff will read the School e-Safety Policy, having had its importance explained, and asked to sign that they have understood its content.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff and technicians that manage filtering systems will have clear procedures for reporting issues to the Head Teacher
- Any complaint about staff misuse must be referred to the Head Teacher.

E-safety Training

- Regular meetings of the computer working group to discuss new technologies, changes in protocol and computing training to keep up to date with emerging technologies.
- An audit of all training needs for current and new staff to improve their knowledge and expertise.
- Regular training for all School staff, either through outsourced courses, or disseminated by members of the computer working party so that they have an insight and awareness of new equipment, software and how to use it.
- Regular access to the Local Authority and Government information on emerging and current computing strategies and protocol.
- Working closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school.
- Survey parents and pupils for their views to develop e-safety strategies.
- Use managed systems to help pupils understand how to manage risk, provide them with richer learning experiences and to bridge the gap between systems at school and the more open systems outside of school.
- Provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies.
- As part of the computing curriculum, systematically review and develop e-safety procedures, including training, to ensure that the school is having a positive impact on pupils' knowledge and understanding.
- Training pupils how to report Internet abuse, pathways to do this and making them aware of all dangers.

I have read the above policy and I accept the terms and conditions of use

Name:

Signature:

Date: