INFORMATION & COMMUNICATION TECHNOLOGY

ONLINE & DIGITAL SAFETY POLICY

Reviewed February 2020
South Wellfield First School
Online & Digital Safety Policy

Contents

Section A Overview

Section B Security and Data Management
- GDPR
- Passwords
- Web Filtering and Virus Protection

Section C Infrastructure and technology
- Pupil Access
- Software/hardware
- Managing the network and technical support

Section D Communication technology
- Mobile Devices
- Social Networks
- School Website
- Instant Messaging
- Virtual Learning Environment (VLE) / NTLP
- Video conferencing
- Use of digital media

Section E Managing the Internet safely

Section F Managing E-mail safely

Section G Managing digital images/videos

Section H Infringements and possible sanctions. Prevent Duty

Appendices
- Starters and leavers Policy
- Pupils Online Safety and ICT Acceptable Use Policy
- Email Acceptable use Policy
- Staff Online Safety and ICT Acceptable Use Policy
This online safety policy is to be read in conjunction with the school ‘Online Safety and ICT Acceptable use – Staff policy’.

Our Online & Digital Safety Policy has been agreed by the Senior Leadership Team (SLT) and approved by Governors. It will be reviewed bi-annually or earlier, as required.

Created by: Mrs L Cardus (Computing Coordinator)

Approved by: Governing Body on 25 February 2020
Section A - Overview

Background/Rationale

ICT is continually developing and new technologies have become a part of everyday life, within and outside of school. These technologies provide interesting and exciting opportunities to develop children’s learning across the curriculum. The National Curriculum states that:

“A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science and design and technology.”

This Online Safety policy has been developed to help ensure that the internet and ICT equipment is used safely, appropriately and in a secure environment. It was revised by the Computing co-ordinator and agreed by staff and Governors.

Recent inspections reported that “Safeguarding is outstanding because the school leads high quality practice and has excellent systems in place to minimise risk to children, for example regular Online Safety training and briefing for parents and carers, staff and pupils.” Also noted that the school “place[s] a high priority on ensuring that pupils are safe, and have maintained the high standards of practice reported on in the last inspection.” This Online Safety policy explains our safeguards and how the school reduces risks, whilst addressing how we teach children and their parents/carers to be responsible users of information communication technology.


The ‘staying safe’ outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for

Policy Aims

- The purpose of this online & digital safety policy is to:
  - Safeguard and protect all members of SWFS 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.

SWFS identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school’s physical buildings.

This Policy document is drawn up to protect all parties – the students, staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

**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.

1. **The technologies**

New technologies are enhancing communication and the sharing of information and are constantly evolving. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- the internet;
- e-mail;
- Video chat;
- Instant messaging, often using simple web cams;
- Twitter;
- Blogs;
- Podcasting;
- Social networking sites;
- Video broadcasting sites;
- Chat Rooms;
- Gaming Sites;
- Music download sites;
- Devices with camera and video functionality;
- Smart phones;
- Tablets/IPads;
- eReaders.
2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at SWFS:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive Online Safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

This policy applies to all members of the school community (including staff, pupils, volunteers, governing body, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school (collectively referred to as “staff” in this policy).

Our Computing Coordinator ensures they keep up to date with Online Safety issues and guidance through liaison with the Local Authority and through organisations such as The Child Exploitation and Online Protection (CEOP). The school’s Computing coordinator ensures the Head, Senior Leadership Team (SLT) and Governors are updated in line with current Government guidelines.

Governors need to have an overview understanding of Online Safety issues and strategies at this school. Governors are aware of local and national guidance regarding Online Safety and are updated on policy developments.

All teachers are responsible for promoting and supporting safe behaviours, in their classrooms and when using technology, following school Online Safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools’ Policy. Staff are reminded and updated about Online Safety matters during training sessions and staff meetings.

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;
- 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 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.
Section B
Security and Data Management

1. GDPR
The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It came into enforcement in the UK on 25 May 2018 and replaces the 1995 Data Protection Directive.

Types of Data
The Information Commissioner’s Office (ICO) define personal and sensitive personal data as:

*Personal data* is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

*Sensitive personal data* is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

SWFS handles and stores information about school staff and pupils and must protect that information. Under the Data Protection Act, you must:
- only collect information that you need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as you need, and only for as long as you need it; and
- allow the subject of the information to see it on request.

SWFS holds both personal and sensitive personal data on staff and pupils. This information is kept for the duration that the individual is at the school and in accordance with statutory guidelines thereafter.

Storing Personal Data

- Network
  Staff and pupils have access to the school network storage. Staff and pupils have individual drives and also have access to the S: Drive where shared documents for learning are stored. In addition, only staff have access to the Z: drive where personal data can be stored. Data can only be held for the period that the person is at the school or is within statutory guidelines. When a pupil leaves the school their network account and personal files are deleted by the school technician and any pupil data and photos/videos are dealt with or deleted in accordance with statutory guidelines.
The Computing Co-ordinator should be consulted when new pupils/staff are to be added to the network.

- Electronic Devices
  Pupil personal data, reports and photos/videos must not be stored on staff portable electronic devices such as laptops and iPads. Personal data should never be put on private computer equipment. Portable devices, such as staff laptops and iPads should be kept as securely as possible on and off school premises. As the school class set of iPads can contain photos/videos of pupils these must be put in the charging trolley and locked in the server room when not in use.

- USB Devices
  USB sticks should not hold personal data unless they are password protected and fully encrypted.

- Paperwork
  Confidential and sensitive data in paperwork format is not to be removed from school premises.

2. 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, they are informed not to write these passwords down at any time. If a pupil or member of staff believe that someone other than themselves has become aware of their password, they are to report to the Computing Co-ordinator or Senior Leadership Team and their password will be changed.

Strong passwords, i.e. at least eight characters long and containing special symbols, should be used if any electronic equipment holds confidential personal information. Different passwords for separate systems and devices should be used and passwords should be changed regularly.

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: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

NTLP Password policy for pupils (Year 3 & 4 only)
Pupils are taught email in Year 3 and are taught about password safety as part of the unit of work. All pupils are taught to change their password. They do not need to change them on any timescale, but are taught through Online Safety lessons that this is recommended.

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 is monitored and can be traced to individual users.
Password Policy statements:
● Always use your own personal passwords to access computer based services.
● Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
● Staff should change temporary passwords at first logon.
● Change passwords whenever there is any indication of possible system or password compromise.
● Do not record passwords or encryption keys on paper or in an unprotected file.
● Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
● Protected data accessed through Citrix users must be changed every term.
● User ID and passwords for staff and pupils who have left the School are removed from the system by the technician.
● If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security
● Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.
● Users are provided with an individual network, email, LaunchPad and Management Information System (where appropriate) login username.
● Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
● Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or LaunchPad, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
● In our school, all ICT password policies are the responsibility of the Headteacher and Computing coordinator and all staff and pupils are expected to comply with the policies at all times.

3. Web filtering and virus protection
Virus protection is purchased for the network and all school computers. Regular scans should be allowed to perform and staff should scan all devices that are not connected to the network, including USB drives.

Any device suspected or found to contain any virus or malware must be immediately turned off and removed from the network. In the event of a virus, note down the details and inform the Computing Co-ordinator as early as possible so appropriate technical support can be sought.
The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Internet filtering is provided by the Local Authority as part of the ICT SLA using the product Smoothwall. 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 (if possible) screen capture the website and report it to the Computing Co-ordinator/Senior Leadership Team and also ict.helpdesk@northtyneside.gov.uk so it can be reviewed and blocked 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 via the proxy 192.168.250.6 port 8000. This has been agreed by Senior Leadership Team 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 in class, this can reduce the risk of students being exposed to unsavoury comments and adverts 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.
Section C
Infrastructure and Technology

Pupil 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.

Software/hardware
All software has been purchased by the school and the school is the legal owner. The dates of appropriate licenses are recorded and kept in a secure cupboard. The school technician loads any new software onto the schools network.

School laptops and iPads are for school use only.

Apps for iPads can be requested by staff using the ‘IPad App Request’ online form. Budget approval must be sort from the Headteacher prior to Apps being requested. Apps can be loaded onto the ‘Teacher’ restricted area or the student access area and in Key Stage folders.

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

All staff should log off or lock a computer when they leave a computer / digital device unattended.

Staff are responsible for ensuring that any computer, laptop or iPad loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.

Managing the network and technical support
The server and cabling is securely located and its physical access is restricted by a password protected door lock. The network is managed by a North Tyneside Technician. The network is monitored via the council.

Staff should not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems, e.g. technical support or SIMS Support through LA systems; Education Welfare Officers accessing attendance data on specific children.

Requests for technical support can be made to support@ntlp.org.uk
Section D
Communication Technology

Use of Communication Technology
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile Devices
We currently do not allow children to bring in or use their own mobile devices in school.

Staff are provided with a laptop and IPad and have access to a school class set of IPads, which are available to all year groups in school, for curriculum use. Acceptable use of the devices are covered in staff and student AUP documents.

Mobile telephones
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. Personal mobile phones should not be used for school activities, e.g: school clubs/trips. It is not acceptable to use personal mobile phones to support lessons. Mobile phones 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.

Social Networks
SWFS has a school Twitter account @southwellfield, which only staff have password access to update. This is only used to update our school community about events happening in school and in the classroom. Staff are requested not to ‘follow’ any users using the school account, but to use their own personal twitter account to interact with others.

Photograph permissions will be sought on a yearly basis. Families can opt in or out of photographs of their child(ren) being used for school purposes, for example on twitter.

Users of social media should consider the 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.

The school will control access to social networking sites. Pupils will use only moderated social networking sites, e.g Seesaw, if appropriate.

Process for creating new accounts
The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-
● The aim of the account;
● The intended audience;
● How the account will be promoted;
● Who will run the account (at least two staff members should be named);
● Will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

**Personal Social Networks**

- 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 where appropriate 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 on any social networking site, unless it is from the school’s official accounts and with the permission of the Headteacher.
- 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.

**School Website**

The school website is www.southwellfieldfs.org.uk. It provides key information to the public about the school and links to the school Twitter account where the school and pupils work is celebrated.

The contact details given online is for the school office. The point of contact on the Website is the school address, school email and telephone number. Staff and pupil personal contact information will not be published

The following members of staff have administrative rights to edit our school website, which is locked securely by individual passwords:

- Headteacher
- Computing co-ordinator
- Business Manager

The Headteacher will take overall editorial responsibility and will ensure that content is accurate and appropriate.

The school website is fully compliant with Government and Ofsted requirements for schools maintained by a local authority.
**Instant Messaging**
Instant Messaging, e.g. Whatsapp, facebook messenger etc, provides an opportunity to communicate in real time using text, sound and video. It is not appropriate to use these tools in school lessons.

**Learning Platform**
Accounts are linked directly to our school’s SIMS database. As pupils are removed from SIMS they are removed from the school. If they move onto a new school the account will be transferred. When they leave the North Tyneside school system their account will be suspended.

**Video conferencing**
Any use of video conferencing/video chats must only take place with the permission of a member of the senior leadership team. Any use of external video conferencing software (e.g. Skype) must not be done with a teacher’s ‘personal’ account. It is good practice to create a separate account for school communications. 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 being viewed in this way. Children should be consulted and adults would need to consent as well as the parents 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 look at the images and what security measures are in place to protect access.

When using video conferencing in the classroom, children will be taught about safe, appropriate and acceptable use of these technologies.

As children also have access to NTLP Google 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 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/twitter.

- 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. Staff are instructed that these images/videos are not to be stored on any personal computers, devices etc.
- 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 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 Computing coordinator and SLT.

**Protecting personal data**

Personal data will be recorded, processed, transferred and made available in line with GDPR.
Section E
Managing the Internet Safely

The risks
The Internet is an open communications channel, available to all. Anyone can send
messages, discuss ideas and publish material with little restriction. These features of the
Internet make it both an invaluable resource used by millions of people every day as well as
a potential risk to young and vulnerable people.

In line with school policies that protect pupils from other dangers, there is a requirement to
provide pupils with as safe an Internet environment as possible and to teach pupils to be
aware of and respond responsibly to any risk.

The school helps protect itself by making it clear to users that the use of school equipment to
view or transmit inappropriate material is “unauthorised” and infringements will be dealt with;
and by ensuring that all reasonable and appropriate steps have been taken to protect pupils.
Reasonable steps include technical and policy actions and an education program for pupils,
staff and parents.

Technology
SWFS is connected to North Tyneside’s Internet Connection. We have Fortinet wireless
access allowing wireless connection to the school’s network for staff and pupil devices as
well as BYOD (Bring your own device). Network filtering is provided by this association.
The school is protected by an onsite firewall as well as the Council’s firewall.
Additionally, up-to-date anti-virus and anti-spyware software is in place on all school
computers and teacher laptops.
Unfortunately, inappropriate materials will inevitably get through any filtering system. So, all
staff members should be vigilant and alert so that sites can be blocked.

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 acceptable and
what is not 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 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 e.g.
including using the CEOP Report Abuse icon.

Policy statements:
South Wellfield First School:

• Maintains connectivity through North Tyneside’s Internet Connection;
- Works in partnership with the LA to ensure any concerns about the system are communicated to North Tyneside so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus and anti-spyware software;
- Never allows pupils unauthorised access to the Internet;
- Pupils will be informed that network and Internet use will be monitored;
- Uses ‘pupil log-in’ application to restrict pupil access to programmes and files;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Uses ‘safer’ search engines with pupils such as http://www.safeshare.tv/ and activates ‘safe’ search where appropriate.

**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 parents/pupils must read and sign the Acceptable Use Policy before using any school ICT resources/Internet;
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems;
- In Early Years, pupils use games on the interactive whiteboard.
- 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;
- This online safety policy will be published on the school website.

**Policy statements:**

**South Wellfield First School:**

- Supervises pupils’ use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the North Tyneside filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use and informs users that Internet use is monitored;
- Plans the curriculum context for Internet use to match pupils’ ability, using child-friendly search engines where more open Internet searching is required;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing Coordinator/ Headteacher. This will in turn be reported to the LA;
- Blocks all Chat rooms and social networking sites except those that are part of educational lessons;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes;
- Requires parent/carers and children to individually sign a ‘Online Safety and internet Acceptable Use Policy’ form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an ‘Online Safety and ICT Acceptable use staff policy’ and an ‘Email Acceptable Use Policy and keep a copy on file;
- Makes clear all users know and understand what the rules of appropriate use are and what sanctions result from misuse – through staff meetings and teaching programme;
• Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
• Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
• Immediately refers any material we suspect is illegal to the appropriate authorities – LA / Police.

Sanctions and infringements
The school’s Internet Online Safety / Acceptable Use policy will be made available and explained to staff, governors, pupils and parents, with all signing acceptance agreement forms appropriate to their role. Sanctions for infringements to the acceptable use policies are clear and available for all staff, governors, pupils and parents. (See Section H)

Handling online safety incidents
Our Computing coordinator acts as 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. (See “How to deal with an online safety incident involving staff” Document attached. https://drive.google.com/file/d/1OOs0qyKoPZDRENQiyC_K9nFD7vBdHa2s/view?usp=sharing

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 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 and passed to relevant personal;
• If necessary the Local Authority will be informed of any misuse and parents will be
● Pupils and parents will be informed of consequences for pupils misusing the Internet;
● Parents 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 then may then involve contact with the police for further advice (at the discretion of the Headteacher).

Parents 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 safeguarding 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)**

● 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 ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.
Staff and the online safety policy

- All staff have access to 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, and the school website;
- 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 Computing coordinator.
- Each incident that takes place will be reviewed by the Computing coordinator and appropriate action will be taken.
- 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.
- AUPs are reviewed annually and updated to include new technologies, when necessary.

Education programme:

Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. Pupils need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or Computing Coordinator for inclusion in the list of blocked sites.

Pupils must learn to recognise and avoid risks online – to become ‘Internet Wise’. To STOP and THINK before they CLICK.

Pupils also need to make good judgements about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet based information. Just because something is published in text or on-line does not make it fact. It is therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that pupils consider whether something is plausible or biased.
Pupils will be accessing reliable material but need to select that which is relevant to their needs, for instance to answer a homework question. Pupils are taught research techniques including how to narrow down searches and how to skim and scan content.

A programme of training in Online Safety has been developed, based on the internet based materials from CEOP, Hector’s world and sites recommended by North Tyneside ICT Team. Online Safety is built into schemes of work, to ensure pupils are ‘taught’ safe behaviours and practice and the school will foster a ‘No Blame’ culture to ensure pupils feel able to report any abuse, misuse or inappropriate content.

Policy statements:
South Wellfield First School:

- Fosters a ‘No Blame’ environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off the monitor/screen and report it to the teacher or Computing Coordinator;
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Has a clear, progressive Online Safety education programme throughout all Key Stages, built on North Tyneside / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
  - to STOP and THINK before they CLICK;
  - to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - to be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know some search engines / websites that are more likely to bring effective results;
  - to know how to narrow down or refine a search;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand good behaviour when using an online environment such as a ‘chat’ / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
  - to not download any files – such as music files - without permission;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
  - to have strategies for dealing with receipt of inappropriate materials;
  - this list is not exhaustive.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures regular Online Safety training and updates are made available to staff;
- Provides advice, guidance and training for parents, including:
- Information in safety leaflets
- Information in school newsletters
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents
- Online Safety awareness training courses
Section F - Managing E-mail Safely

How will E-mail be managed?
The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, unregulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, email is not considered private and is monitored, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

Staff and pupils may only use approved e-mail accounts on the school system. All users have access to the NTLP Google mail via our VLE (North Tyneside LaunchPad) and will be migrating to Microsoft 365.

All NTLP Gmail is filtered. Email content, titles, addresses and attachments are scanned for questionable content, which is defined by LA admin staff for NTLP. 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 pupil level data or personal data sent over the Internet must be encrypted or only sent within the approved secure system in our LA. NTLP email is insecure and not to be used to send critical data.

Education:
As North Tyneside LaunchPad requires users to have an email account to login, 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 once they reach key stage 2 (year 3) and this is used in Computing lessons only. Pupils are made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This is part of the school’s Online Safety education programme. Pupils in key stage 2 are taught to use e-mail appropriately and safely.

Policy statements:
South Wellfield First School:

- Does not publish personal e-mail addresses of pupils or staff;
- Uses group e-mail addresses, as appropriate;
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.

Pupils:
NTLP passwords must be at least 6 characters for primary aged pupils. There is no requirement to change them on any timescale, but talking about good passwords and changing them periodically is taught as part of online safety lessons as they progress through school.

- 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;

The school should consider how email from pupils to external bodies is presented and controlled;

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.

Pupils and parents/carers sign the school ‘Pupil ICT, Online safety and Internet Acceptable Use Policy’ to say they have read and understood the Online Safety rules.

Staff:

- Staff are expected to check their email mailboxes regularly;
- 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;
- Staff are required to add a standardised email signature covering Name, Role in school and contact details. To do so staff can click on the cog in the top right, then ‘settings’, then scroll down to signature where the passage can be pasted in and details added;
- Staff sign the ‘Acceptable Email Use’ agreement to say they have read and understood the online safety rules, including email, and we explain how any inappropriate use will be dealt with;
- 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.
Section G
Managing digital images/videos

Use of still and moving images
Strict procedures must be followed when using photographs or video footage of pupils, for example when publishing on the school website/twitter. Use group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school.

If showcasing examples of pupils work consider using only their first names, rather than their full names. Only use images of pupils in suitable dress to reduce the risk of inappropriate use. Pupils should be advised why photographs are being taken for official school use when they are to be stored electronically alongside other personal data.

Parental permission must be obtained before publishing any photographs, video footage etc of pupils. This ensures that parents are aware of the way the image of their child is representing the school.

(Publishing refers to sharing any images/video on school website or twitter or via other appropriate means)

Procedures:
Use excerpts of pupils’ work such as written work, scanned images of artwork or photographs of items designed and made, allowing pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Text written by pupils should always be reviewed before publishing it. Make sure that the work doesn’t include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils’ work doesn’t contain any statements that could be deemed defamatory.

Ensure that the school is not infringing copyright or intellectual property rights through any content that is published. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video.

Technical:
Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

When saving pictures, ensure that the image file is appropriately named. Do not use pupils’ names in image file names or in <ALT> tag references when published on the web. [An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]
If using video as part of a lesson, it is important that staff do not use software to ‘rip-out’ sections of copyrighted movies without permission.

**Education:**
We ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils are taught to understand how to consider an external ‘audience’ when publishing or presenting work.

**Policy statements:**
South Wellfield First School:

- Digital images/videos of pupils are only to be stored on password encrypted USB drives or on the password protected teacher’s area on the school network (not teacher laptops). Images are to be deleted at the end of a school year, unless an item is specifically kept for a key school publication;
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author’s identity or status;
- We gain parental/carer permission for use of digital photographs or video involving their child, as part of the school agreement form;
- We do not use pupils’ names when saving images in the file names or in the <ALT> tags;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are not permitted to publish any material online without strict supervision of a member of staff;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT work;
- Pupils are taught about how images can be abused in their Online Safety education programme.
Section H - Infringements and possible sanctions

Assessing risks
At South Wellfield First 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 computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

We 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 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 Anti-bullying policy.

Incidents related to child protection are dealt with in accordance with the school’s child protection policy. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to the Headteacher immediately.

If an incident occurs involving a pupil, the member of staff in charge must seek the nearest member of staff so they can witness the misuse, protecting them 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 instructed in different types of Online Safety incidents and are aware that they must report them immediately. Once incidents are reported, a record must be made by the member of staff involved. One of the designated members of staff will inform how to deal with the incident.

If necessary the Local Authority will be informed of any misuse and parents will be informed. Pupils and parents will be informed of consequences for pupils misusing the Internet. Parents and pupils will need to work in partnership with staff to resolve issues.

As with other safeguarding issues, there may be occasions when the 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).
How will infringements be handled?
Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

**Pupils**

**Category A infringements**
- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile devices (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Sanctions: referred to class teacher / senior manager / Computing Coordinator]

**Category B infringements**
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile devices (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. BitTorrent etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Sanctions: referred to Class teacher/ Key Stage Leader / Computing Coordinator / removal of Internet access rights for a period/ contact with parent]

**Category C infringements**
- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email or instant message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Sanctions: referred to Class teacher / Key Stage Leader / Computing Coordinator / Headteacher / removal of Internet and/or LaunchPad access rights for a period / contact with parents / removal of equipment]

**Other safeguarding actions**

If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site
2. Inform LA as appropriate

Category D infringements

- Continued sending of emails messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act or GDPR.
- Bringing the school name into disrepute

[Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer / LA Online Safety officer]

Other safeguarding actions:
1. Secure and preserve any evidence
2. Inform the sender’s e-mail service provider
Incidents involving staff
Any incident involving staff misuse must be referred immediately to the Headteacher. It is fully recognised that an authorised staff user may accidentally breach this policy whilst acting in good faith and in the course of their duties. If a member of staff suspects this may be the case they must notify the Headteacher or Computing 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 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.

Staff

Category A infringements (Misconduct)
- Use of Internet for personal activities not related to professional development e.g. online shopping, personal email, messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software.

[Sanction - referred to line manager / Headteacher. Warning given.]

Category B infringements (Gross Misconduct)
- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act or GDPR.
- Bringing the school name into disrepute.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police]

Other safeguarding actions:
- Remove the PC to a secure place to ensure that there is no further access to the PC, laptop or portable device.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

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

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

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): [http://www.ceop.gov.uk/](http://www.ceop.gov.uk/)

**How will staff and students be informed of these procedures?**

- They will be fully explained and included within the school’s Online & Digital Safety Acceptable Use Policy and all staff will be required to sign the policy.
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop ‘safe behaviours’. Pupils and parents/carers will sign an appropriate Online Safety Acceptable Use form.
- The school’s Online Safety policy will be made available to parents/carers on the school website.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents/carers.

**Incidents involving other adults (e.g. parents)**
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 then involve contact with the police for further advice (at the discretion of the Headteacher).

**How will complaints regarding Online Safety be handled?**
The school takes all reasonable precautions to ensure Online Safety. 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 computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
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, which states that they must have ‘due regard to the need to prevent people from being drawn into terrorism’. Issues and policies relating to this are covered in our school safeguarding policies, but we are 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 we strive to keep our young people safe and minimise risks they face while they engage with technology in our care.

Statutory Guidance from the Government can be found in the following publications:

The Prevent Duty
Appendices
Starters and Leavers Policy

What to Do When a Teacher/ Staff member Leaves.

The purpose of this section is to:

- Help ensure that a 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 will 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 the 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** – account disabled but not deleted. (Details to be sent to the Computing Coordinator), **Email** – disable password.
Pupils Online Safety and ICT Acceptable Use Policy

South Wellfield First School provides ICT equipment and internet access to support learning.

To stay safe when we use ICT equipment and the internet I agree that:

- I will only use school ICT equipment for school use when I have permission from a staff member.
- I will take care of the computer and other equipment that I use and will report any damage or faults, however this may have happened.
- I understand that I should not write down or store a password where it is possible that someone may take it. I will not tell anyone my password or use someone else's password.
- I will be aware of “stranger danger” when I am communicating on-line and will not give out my personal information. This includes my name, email, telephone number, home address or the school I go to. I will check with a grown up if anyone wants to know these things about me.
- I will be considerate of others and will be polite, responsible and sensible in all of my ICT use.
- I will not take, store or share images of anyone without their permission and without the permission from school staff.
- I will respect the privacy and ownership of others’ work online.
- If I see something that worries or upsets me, or makes me feel uncomfortable, I will tell a member of staff straight away.
- 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.
- KS2 - I understand that others may read or share email messages I receive or send. I will only email people I know and that my teacher has approved and checked.
- KS2 - 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 understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, my computer rights revoked and my parent/carer contacted.

Please detach and return the signed agreement below.

Pupil ICT, Online Safety and Internet Acceptable Use Policy

Child’s Name: ___________________________________       Class: ______________________

For Children
I have read and understand the school ICT rules and agree to comply with this policy. I promise to be a safe and sensible Internet User.

Signed: ______________________________________ (Child)       Date: _____________

For Parents
I have read and understand this policy and have discussed it with my child. I give consent for my child to have supervised access to Internet resources.

Signed: ______________________________________ (Parent/carer)       Date: _____________

Parents name (Please print) ____________________________________________
Email Acceptable Use Policy

(This part of the policy is applicable to all users who have NTLP email access via the Learning Portal).

I understand:

• That all electronic communications made through NTLP & Microsoft 365 and its systems are the property of North Tyneside Council.

• That certain communications are illegal (for example, sending child abuse images, harassing or malicious messages, hacking someone else's account, incitement to racism etc) and will be followed up by the appropriate authorities.

• That NTLP communications have filtering systems in place; filtered messages are quarantined for investigation.

• That if I do not keep to this policy, my actions may be investigated.

• That unacceptable behaviour may lead to sanctions or disciplinary action as appropriate.

I Agree:

• To comply with all legal requirements concerning digital communications.

• To respect others: communications and other content I post will be polite and considerate in tone and content.

• To ensure all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA. NTLP email is insecure and not to be used to send critical data.

• To keep up-to-date with training and policies on the use of these technologies as provided by the school.

• Not to reply to offensive or upsetting communications, but to report them to a manager.

• Not to open suspicious attachments as they may contain a virus.

• Not to send chain messages or spam mail.

• Not to enter into any contracts or financial arrangements on behalf of school or organisation without suitable authorisation.

• To do my best to be safe online (see www.thinkuknow.co.uk)

• Not to put myself or others at risk by giving away personal details.

Signed: ___________________________ Print Name: _________________________ Date: ______________
South Wellfield First School

Online & Digital Safety and ICT Acceptable Use

Staff Policy

February 2020
Introduction

South Wellfield First School strongly believes in the educational value of ICT and recognises its potential to enable staff in delivering and supporting the curriculum. South Wellfield First School also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of the School is that staff will play an active role in implementing online safety and acceptable use through effective classroom practice.

This policy applies to the school governing body, all teaching and other staff, whether employed by the Local Authority or employed directly by the school, external contractors providing services on behalf of the school or the Local Authority, teacher trainees, other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

Online and digital safety is about ensuring that you, as a member of staff at the School can use the Internet, email and other technologies available at the school in a safe and secure way. This policy covers the use of ICT systems, the use of telephones, online tools, email and the internet provided by the School to support learning. It also extends to out of school facilities e.g. equipment; printers and consumables, managed learning environment, social media and websites (where applicable).

The School recognises that for staff to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the School and have the opportunity to expand and develop the teaching material associated with their work. However, the School expects that all staff, will at all times, maintain an appropriate level of professional conduct in their own use of the School’s ICT facilities. All electronic communications with pupils and staff must be compatible with your professional role.

Listed below are the terms of this agreement. Staff are expected to use the ICT facilities of the School in accordance with these terms. Violation of these terms will result in disciplinary action in accordance with the School’s Disciplinary Procedures.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

All computers and associated equipment are the property of the School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990, General Data Protection Regulation and the Data Protection Act 2018. The School assumes responsibility of maintenance of all hardware and software. Misuse of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading of computer viruses or other malware
- Deliberate deletion of files
- The uploading of inappropriate computer files to the School’s network.
The above actions can reduce the availability and reliability of computer equipment, put data at risk and increase downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

**IPads, Laptop Computers and devices**

Laptop computers are issued to all teaching staff and support staff as required. These devices remain the property of South Wellfield First School at all times, and their usage is subject to the following guidelines:

- The equipment remains the property of the School at all times.
- Maintenance of the equipment is the responsibility of the School.
- All installed software MUST be covered by a valid license agreement held by the School or its ICT provider.
- All software installation MUST be carried out by ICT technician in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. This should be done at least weekly.
- Any external devices, eg: card readers, pen drives, USB disks, data CD’s should be scanned with anti-virus/spyware before use.
- In the event of a virus isolate the effective device from the network and note down the details and inform the computer co-ordinator/technician as early as possible.
- The user of the equipment is responsible for all personal files and data stored on the equipment.
- Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the school’s facility to transfer files is used.
- The School cannot be held responsible for loss of personal data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for the ICT technician to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.
- Photographs/videos and school related data about children are not to be kept on laptops/ipads.
- Equipment should be carried in the appropriate laptop bags provided by school.
- Where equipment is damaged this must be reported to the Headteacher. Damaged equipment may not be replaced.
- When portable devices are taken off the school premises, they must be kept securely.
- Staff are not permitted to use personal mobile phones for school use (see section 6)

**Use of Removable Storage Media**

Staff have been provided with encrypted USB sticks for reports and other school related data. Memory sticks to transfer files between home and school should be password protected and encrypted. They should not be used as the sole means of storage for important files.
Printers and Consumables

Printers are provided in the School for educational or work-related use only. All printer usage will be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proof-read your document on-screen and use the ‘Print-Preview’ facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

Data Security and Retention

All data stored on the School network is backed up daily. If you should accidentally delete a file or files in your folder or shared area, please inform the Computing Co-ordinator or ICT Technician immediately, so that it can be recovered.

2. Internet and Email

The School provides Internet filtering, designed to remove controversial, offensive or illegal content. It is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report this to the Computing Co-ordinator so appropriate action can be taken.

Access to the internet is available at any time, except during outages and essential maintenance periods.

Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- Staff have a responsibility to investigate the websites that pupils will be using before a lesson.
- If pupils are using the internet in your lessons, it is your responsibility to ensure they are appropriately monitored and that only pupils who have written parental permission to use the Internet are allowed to do so.
- If you ask a parent or student teacher to work with pupils, you must make sure they are familiar with the acceptable use policies for staff and pupils when using the Internet.
- Do not infringe copyright and intellectual property rights. If you are in doubt or cannot obtain written permission from the copyright holder, do not download or copy the material concerned.
- Transmission of any material in violation of any United Kingdom or other national law is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- The use of Internet chat sites is prohibited.
• The use of online gaming sites is prohibited.
• Downloading or installing software from the Internet is not permitted.
• Staff are reminded that ALL Internet access is logged and actively monitored.

Email

To be read in conjunction with SWFS ‘Email Acceptable Use Policy’.

Where Staff are provided with an email address this may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the School retains the right to monitor email communications at any time, if this is deemed necessary.

• The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.
• Messages relating to, or in support of any illegal activities will be reported to the relevant authority.
• Attachments received on an email should not be opened unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the School network.
• Staff email is insecure and not to be used to send critical data.
• Where digital personal data is transferred outside the secure local network, it must be encrypted. An encryption service is an option if you do not have encryption enabled on emails. An encryption service enables you to send documents in a safe and secure manner. These work by sending the recipient an email with a secure link to a repository where the associated document(s) can be downloaded over a safe connection. An encryption service also provides a full audit trail and logging of all emails and their attachments.
• Verify the details, including accurate e-mail address, of any intended recipient of the information
• Send the information as an encrypted document attached to an e-mail
• Provide the encryption key or password by a separate contact with the recipient(s)
• When sending emails externally to more than one person, you must hide the recipients’ email addresses. You can do this by putting just your own name in the “To” field, and putting the other addresses in the “Bcc” field.

3. Privacy and Data Protection

Passwords

• Comply with the ICT system security and do not disclose any passwords provided by the school or related authorities.
• Never share your password with anyone or ask others for their password.
• When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name. It is advisable to use a ‘strong’ password, which contains a combination of upper and lower-case letters, numbers and other punctuation characters. Current Government guidance is that a phrase should be used that is familiar to you e.g. W1ndinth3w1llows
• If you forget your password, please request that it be reset via your ICT technician
• If you believe that your password has been compromised, change it immediately.
4. **Security**

- Never attempt to access files or programs for which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection legislation and such attempts will be subject to disciplinary action.
- Never grant or allow access to files or programs to unauthorised users. This is a breach of school policy and data protection legislation and such attempts will be subject to disciplinary action.
- Any security concerns should be reported immediately to ICT.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with the School Disciplinary Procedures.
- 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.

5. **Access to the School network & school devices**

Access to the School network is available to those staff who require it. Access is subject to agreement and is subject to the following guidelines:

- Password security is vital. If you believe that your password has been compromised change it immediately.
- If you leave your computer unattended, particularly in a classroom, you must lock it by using the ‘Windows and L key’.
- If you are connecting to an interactive whiteboard and projector, please be aware that any pupil information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, please ensure that projectors are turned off or disconnected before connecting.
- The Clevertouch interactive screens can be managed using the remote control. Blue button – freeze screen, Yellow button – stops interactivity and Red button – Lock.
- Never perform ‘live’ (in front of the class) web or image search during a lesson. Despite security filters in search engines, inappropriate material can still be shown. Best practise is to find the image or website before the lesson.
- When working from home Staff must ensure that their home Internet connection is secure from outside access particularly if a wireless network is used. Additionally staff should take due care regarding who may potentially have access to the PC or any material which may be printed at home.

6. **Mobile Phones**

Staff should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person. Mobile phones are not to be used within the classroom or when pupils are present. Phones should be turned off or on silent during lessons. Personal mobile phones should not be used for school activities, eg: clubs/trips or taking photographs etc.
7. Digital Photographs/videos

- 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.
- Digital photographs or videos are only to be taken of children for which parental/carer permission has been given.
- Photographs/videos published on the school twitter account @southwellfield or the school website www.southwellfieldfs.org.uk should not have full names of children attached.
- Digital images/videos of pupils are only to be stored on password encrypted USB drives or on the password protected teacher’s area on the school network (z: drive), not on teacher laptops. Images are to be deleted when a child leaves the school, unless an item is specifically kept for a key school publication or event.

Online Safety and ICT Acceptable Use Staff Policy

If you come across anything, whether in an email, a web page or during a video conference, that you consider inappropriate or breaks the acceptable use policy, switch off the computer monitor or screen, and immediately inform the Computing Coordinator or Headteacher as soon as possible.

MEMBER OF STAFF:

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 understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action being taken against me. I agree to use the School ICT systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

NAME (Please Print): ________________________________   Date : __________

SIGNATURE: ______________________________________________
Online Safety and ICT Acceptable Use Staff Policy

If you come across anything, whether in an email, a web page or during a video conference, that you consider inappropriate or breaks the acceptable use policy, switch off the computer monitor or screen, and immediately inform the Computing Coordinator or Headteacher as soon as possible.

MEMBER OF STAFF:

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 understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action being taken against me. I agree to use the School ICT systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

NAME (Please Print): _____________________________   Date : __________

SIGNATURE: ______________________________________________