Swalwell Online Safety Policy

Review Date	Changes made	By whom	Date Shared
March 2020	Yes	AHT KM	March 2020
Sept 23			

Introduction

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Swalwell Primary's activities.

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.
(See also appendix 3 – Incident work flow)

Rationale:
The potential that technology has to impact on the lives of all people increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than adults. In many areas, technology is transforming both the way schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we help those who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

The Law
This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Our Online Safety Policy has been written by the school, using advice from Gateshead LA, and government guidance. The Policy is part of the School's Improvement Plan.
Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Roles and Responsibilities

All at Swalwell Primary are committed to safeguarding children in our care. This policy has been developed by the Online Safety / Computing Lead and the Senior Leadership Team in order to ensure that it truly reflects our robust and thorough approach to safeguarding. This section outlines responsibilities of staff, leaders and stakeholders as well as all users of technology within school.

Role	Key Responsibilities
Head of school	To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security GDPR compliant • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL • To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious Online Safety incident. • To receive regular monitoring reports about Online Safety from Computing Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures
Online Safety – Computing Co-ordinator / Designated Child Protection Leader	takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that Online Safety education is embedded across the curriculum • liaises with school COMPUTING technical staff • To communicate regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online Safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: •

	sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media To oversee the delivery of the Online Safety element of the Computing curriculum • To address Online Safety issues as they arise promptly
Governors	To ensure that the school follows all current Online Safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in Online Safety activities Adhere to the acceptable use agreement when in school Have due regard for the importance of Online Safety in school
Network Manager/technician The school uses third party company – Gateshead Computer Services for technical support	To report any Online Safety related issues that arises, to the Computing Coordinator/SLT. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school Computing system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • Gateshead LA is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's Online Safety policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant • that the use of the network / remote access / email/School Twitter account is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator/Data Protection Lead /Head of School for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Protection Lead/ Data Protection Officer	To take overall responsibility for data and data security • To ensure that all data held on pupils on the school office machines have

	appropriate access controls in place
Teachers	To embed Online Safety issues in all aspects of the curriculum and other school activities To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	To read, understand and help promote the school's Online Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Online Safety coordinator • To maintain an awareness of current Online Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • Keep passwords private and only use their own login details, which are stored securely • Monitor and supervise pupils' internet usage and use of other IT resources • Adhere to the Acceptable Use Agreement • Promote Online Safety and teach Online Safety units as part of computing curriculum • Only download attachments/material onto the school system if they are from a trusted source • When capturing images, videos or sound clips of children, only use school cameras or recording devices • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.

	• To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's ESafety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/ review of Online Safety policies
FamilyLiaison Officer	Educating Parents and raising awareness as instructed by Computing Coordinator
Parents/Carers	To support the school in promoting Online Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and adhere to the school Twitter policy • To read, understand and promote the school Pupil Acceptable Use Agreement with their children To access the school website /Twitter account accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External Groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school • To seek parental consent if the external party intends to use pupil photograph

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Teaching and Learning

The school will actively teach Online Safety at an age-appropriate level. The school follows a scheme of work for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics. Online Safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (illegal - The Protection of Children Act 1978).

- Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).
- Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business.
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour management procedures.

Monitoring safe and secure systems

Internet access is regulated by Gateshead LA supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, ie use of strong passwords. If personal data has to be saved to other media, eg data sticks or CDs, it is to be encrypted or strong password protected. Staff with access to
the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.

Safe use of the Internet and Web Filtering

- The filtering of internet content provides an important means of preventing users from

accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

- All staff and pupils will have access to the internet through the school's network.
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to Gateshead LA
- If an adult finds a site that they consider unsuitable they should report it to the Online Safety officer and/or Headteacher

The use of Email

Access to email is provided for all staff in school via Microsoft Outlook and office365 email systems. These official school email services may be regarded as safe and secure and are monitored.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary.
- Staff emails should never be used to forward 'chain' or 'junk' email.
- Staff should not communicate with pupils via email.

The school website

The school web site complies with statutory DfE requirements. Our website is for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the school website. Photographs are posted but never include names alongside an image to identify a pupil. Full names are only used when no image could identify specific pupils. Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking, Social Media and Personal Publishing (blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, eg Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home. School and class blogs are run through the school website and are password protected.

Staff private use of social media

- No reference should be made in social media to students / pupils, parents /carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community

- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The use of cameras, video and audio recording equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Assistant Headteachers, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

Use of digital and video images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission.

Personal mobile phones and mobile devices

(See also Mobile Phone Policy)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. Devices should only be used by members of staff in areas not accessed by pupils and only when not in contact with pupils. Staff can, however, request permission to keep a phone switched on in certain circumstances (e.g. an expected and important phone call).
- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- Mobile phones must be kept securely out of the view of pupils unless when being used in the above areas.
- Staff should never use their own personal mobile devices to take or store photographs of children at school events, sporting trips or excursions. Only authorised school cameras and iPads can be used to record videos or images of school events.
- Older pupils are permitted to bring their personal hand held devices into school with the agreement of parents (usually to facilitate the process of children beginning to walk home alone).

All pupil phones are kept locked away during the school day and are collected by children before they leave.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Management of online safety incidents

- There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. Gateshead LA, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Working in Partnership with Parents

Parents' attention will be drawn to the Online Safety policy through the school newsletters, information evenings and on the school website. A partnership approach with parents will be encouraged. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement at the beginning of each year.

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding

(See also Safeguarding and behaviour policies)

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic

devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance

Appendix 1: Pupil and Parent Acceptable Use Agreement
Appendix 2: Staff and Volunteer Acceptable Use Agreement and Policy
Appendix 3: Incident Workflow

Swalwell Primary School
ICT Pupil Acceptable Use Agreement and Online Safety Rules

- I will log on using my own name and password

- I will tell an adult straight away if something on the computer has upset me or worried me so if I find anything or anyone online that makes me feel uncomfortable, unsafe or uneasy in any way, I will tell an adult immediately.

- I will be polite and friendly to everyone I speak to on the computer so I will make sure that all online contact with other children and adults is responsible, polite and sensible.

- I will only send pictures, videos or words that are kind and friendly so I will only upload or add images, video, sounds or text that are appropriate, kind and truthful and will not possibly upset someone.

- I will not tell anyone on the computer my name, how old I am or where I live so I will keep my personal details private when I'm online.

- I know that my teachers will always check to see if I'm being friendly and sensible on the computer and the internet and they will speak to my parents and carers if I am not.

- I will behave sensibly when I'm on the computer because I'm responsible for the way I behave online, and I know that these rules are to keep me safe.

Think before you click!

Dear Parent/ Carer
ICT, including the internet, email, digital and mobile technologies has become an important part of learning in our school. We expect all children to act safely and be responsible when using any ICT. Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your class teacher.

Parent/ carer signature
We have discussed this and ……..(child name) agrees to follow the Online Safety rules and to support the safe use of ICT at Swalwell Primary School.

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

Swalwell Primary School
ICT Staff and Volunteer Acceptable Use Agreement and Online Safety Rules

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my Professional and Personal Safety

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, iPad, email out of school)
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username or password
- I will report immediately any illegal, inappropriate or harmful material or incident
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so
- I will not use social networking sites in school unless it is part of the school curriculum
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities or the reputation of the school
- When I use my personal handheld/external devices in school (laptop, mobile phone, USB devices etc), I will follow the rules set out in this agreement in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will only open attachments to emails if the source is known and trusted. I will not try to access, download or distribute any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install or copy programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without the specific permission of the Headteacher

- I understand that the data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. I will use and encrypted memory stick or save on the school system

When using social networking sites and email outside of school

I understand that I have a professional responsibility when using social networking sites for personal use. As such I will refrain from making school related comments on social networking sites and under no circumstances will I refer to children, parents or staff on social networking sites

I will never use social networking sites to communicate about school related issues and should anyone attempt to make contact regarding a school matter I will refer them to the appropriate channels via school rather than answering directly

I will never run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

I will never maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

I understand that I am responsible for my actions in and out of school

- I understand that this Acceptable Use Policy applies not only to my work and understand that use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement I could be subject to disciplinary action.
- I have read and understand the above, and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed---------- Date----------

Incident Workflow