Summerfields

PRIMARY SCHOOL

E-Safety Policy

Reviewed: **January 2019**

Next Review: **January 2020**

Signed:

SUMMERFIELDS PRIMARY SCHOOL – E-SAFETY POLICY

This policy should be read in conjunction with our Child Protection, Safe Guarding, Mobile Device and Behaviour and Discipline policies.

RATIONALE:

All the governors and staff at Summerfields Primary School are committed to sharing a common objective to help keep the children and staff of the school safe. We ensure that consistent effective safeguarding procedures are in place in order to support families, children and staff of the school.

AIMS:

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of contexts to promote effective learning.

The use of these exciting innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- 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 the social and emotional development and learning of the child or young person.

Many of these risks reflect situations in the off-line world, as with all other risks, it is impossible to eliminate risks completely. It is therefore essential to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This E-Safety Policy explains how we intend to do this, while also addressing wider educational issues in order to help children (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

DEVELOPMENT, MONITORING AND REVIEW OF THIS POLICY:

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Pupil Council
- Full Governing Body and Leadership and Management Committee meetings
- School website and newsletter

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys/questionnaires of pupils, parents/carers and staff

SCOPE OF THE POLICY:

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers the Head Teacher, to such extent as 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this and associate policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

ROLES AND RESONSIBILITIES:

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head Teacher and Senior Leaders:

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Subject Leader.
- The Head Teacher is responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Head Teacher and Senior Leaders should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Computing Subject Leader:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and review the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school IT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant staff and Governor meetings.
- Reports regularly to the Head Teacher.

The IT Technician is responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined by any relevant Local Authority E-Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

- That the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher and Computing Subject Leader for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current E-Safety Policy and practices.
- They have read, understood and signed the school staff Acceptable Use Policy. Appendix A.
- They report any suspected misuse or problem to the Head Teacher/Computing Leader for investigation/action/sanction.
- Digital communications with pupils should be on a professional level and, where possible, carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school E-Safety and Acceptable Use Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor computing activity in lessons, extra-curricular and extended school activities.
- They are aware of e-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.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection:

Should be trained in e-safety issues 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

Pupils:

- Are responsible for using the school IT systems in accordance with the Pupil Acceptance Use Policy (Appendix B) which pupils are expected to sign before they are given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers must play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand potential issues through newsletters, letters, the school website and information about national/local e-safety campaigns and presentations/courses. Parents and carers will be responsible for:

- Endorsing (by signature) the parental permission for internet access and responsible use of the internet form. Appendix C

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need to help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of Computing/PHSE/other lessons and will be regularly revisited – this will cover both the use of IT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of IT, the internet and mobile devices.

The following E-Safety skills should be taught within IT lessons:

Year 1 & 2	Year 3 & 4	Year 5 & 6
• I can recognise advertising on websites and learn to ignore it • I can follow the school rules when being online and using technology • I know that personal information should not be shared online • I know how to report something bad that I find online • I know who to tell if I find something bad online • I understand what cyber bullying is and what to do if it happens	• I can create a strong password and understand who I must and must not share it with • I know that websites sometimes include pop-ups that take them away from the main site, including the use of advertising • I understand the need for rules to keep me safe when using technology when online and can follow my own and the school's rules • I understand the need to keep personal information private and recognise that everything I put online can be seen and used by others and cannot be deleted • I understand the need for caution and know how to respond if something happens I am uncomfortable with • I can recognise that cyber bullying is unacceptable and the consequences of taking part in it • I know how to report an incident of cyber bullying • I understand the benefits of developing a "nickname" for online use	• I can create a strong password and manage them so that they remain strong • I understand that copyright exists on most digital content and understand they should not publish other people's pictures or tag them on the internet without permission • I can reference information sources • I recognise the potential risks of using technology and know-how to minimise those risks (including identifying people who can help, minimising the screen, reporting systems both online and in school and creating online alias) • I can use my understanding of the internet and technology to create tips to help others use them safely, including dealing with cyber bullying • I appreciate that everything I put online may be seen and used by others and cannot be deleted • I understand that online environments have security settings, which can be altered, to protect us • I can discuss the positives and negatives of IT in my own and the lives of others

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Computing Subject Leader will provide guidance/training as required to individuals as required
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any working group involved in IT/e-safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.
- School IT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school IT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems.
- All users will be provided with a username and password by the IT technician who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.
- The "administrator" passwords for the school IT system, used by the Network Manager must also be available to the Head Teacher and kept in a secure place (eg school safe).
- Users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Internet access in the school is provided via a broadband link which is filtered, access is then blocked to any material which is not felt to be appropriate.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or any user, this must be logged and carried out by a process that is agreed by the Head Teacher (or other nominated senior leader).
- Any filtering issues should be reported immediately by the Network Manager.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the IT Subject Leader.

- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Subject Leader or Head Teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of IT across the curriculum.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material access on the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school

will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 eg social networking, Facebook, X-Box Live, messaging – SnapChat, Instagram, Vine, WhatsApp etc.
- Staff are allowed to take digital/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 taken on 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.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs unless specific permission from parents has been granted.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media (as part of the Acceptable Use Policy signed by parents or carers).

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communication technologies

Mobile Phones

The use of mobile phones will not be permitted during lessons or formal school time by staff or pupils. This excludes occasions when staff may need to use mobile phones, for example on school trips, or as part of a demonstration in a lesson. Staff may use their mobile phones in the staff room outside of formal school time but they must not be taken into class without the express permission of the DSL or Deputy DSL and not be used for personal reasons during the time staff are with children.

School Website

The school website is maintained and kept up to date by the Head Teacher, the IT Technician and administration staff. The Head Teacher ensures that the content on the school website is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website.

Social Networking

The use of public online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils. Thus public social networking sites and newsgroups will be blocked and filtered. Pupils are advised never to give out any personal details that might identify them or their location. Pupils are advised never to give out any personal details that might identify them or their location. Pupils are advised not to place personal photos on any social network space. Pupils are advised on security and encouraged to set passwords and deny access to unknown individuals. Pupils are advised never to agree to meet someone they have met on a social networking site. Should pupils have any concerns about social networking sites or chat rooms, they are advised that they must tell an adult.

Staff must not publish children's surnames on school social media sites. Only children whose parents have given specific written consent may be posted on school social media sites. When posting on social media sites such as Facebook, staff must not

give details of exact locations where children can be found for event outside of usual school days and times.

Email

- Curriculum activities that involve the use of email will be delivered through email programmes that are controlled by the school and only use accounts that are approved by the school.
- The use of individual pupil personal accounts will not be permitted through the school system.
- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – 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.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Responding to incidents of misuse

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school E-Safety Policy. It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless, irresponsible or, very rarely, deliberate misuse. The Head Teacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored. If members of staff suspect that misuse might have taken place, they should be referred to the Head Teacher. It is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. 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.

Appendix A

Summerfields Primary School

Acceptable Computer Use and Internet Access Policy for Staff

The computer system is owned by the school, and may be used by staff to further their role. The school's Computer Use and Internet Access Policy has been drawn up to protect all parties – the pupils, parents, the staff and the school.

The school also reserves the right to examine or delete any files that may be held on its computer system and to monitor all aspects of any live computer use or Internet sites visited without staff knowledge or permission.

- All computer use and Internet activity should be appropriate to the member of staff's employment
- Access should only be made via your authorised account and password from an authorised computer system, which should not be made available to any other person
- Activity that threatens the integrity and security of the federation's ICT system, or activity that attacks or corrupts other systems, is forbidden and is a criminal offence
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- As e-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the school's computer system for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected; as a general rule if you think that in normal circumstances materials would be paid for, then using a computer and/or the Internet to obtain it is likely to be a breach of copyright which can lead to being taken to court
- Posting anonymous messages, network messages and forwarding chain letters is forbidden
- Use of the school's computer system to access inappropriate materials such as pornographic, racist or other offensive materials is forbidden
- Great care should be taken with giving out personal details such as addresses, telephone numbers, bank details etc on Internet sites
- Personal contact details should never be given out in unregulated situations like chat rooms
- Both the Data Protection Act 1997 and the Computer Misuse Act 1990 apply to staff and student use of the computers. Copies of these pieces of legislation are available on request or can be viewed through the hyperlink when logging on to the computer system
- If staff are caught misusing the computer network, the school is obliged to take action according to the severity of the offence
- Cyberbullying is considered an offence and will result in the same sanctions as other staff bullying incidents
- The following activities are examples (but not an exhaustive list) of things which could lead to punishment by the school or even investigation by the police;

1) Using messenger or chat programs on the federation site
2) Downloading or running software (even free or shareware programs) from the Internet or brought in from home
3) Using or attempting to use another person's log-in number and/or password
4) Searching or attempting to access information, files or folders not allocated to you or that are hidden from you
5) Attempting to connect any other piece of computer hardware to the federation's computer network either by any means without permission

- The following items are unlikely to be acceptable for connecting to the network; laptops, palmtops/PDAs, mobile phones or any other intelligent device
- The following items may be acceptable for connecting to the network however you should seek permission prior to using; USB based Flash or disk drives, digital cameras, MP3 players
- If you are in doubt about the acceptability of something which you are about to do on the computer you should seek the advice from the Head Teacher.

By signing this document you are showing that you understand and agree to all of the policy terms.

Signed: _____ Full Name: _____ Date: _____

Appendix B

Summerfields Primary School
Pupil Acceptable Use Policy

Rules for Responsible Internet Use

The school has a range of devices which provide Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- I will ask permission from a member of staff before using the Internet.
- I will not access other people's files.
- I will use the computers only for school work and homework.
- I will not bring personal storage into school unless I have permission.
- The messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will use the computers sensibly and responsibly at all times.

Pupil's agreement

I agree to follow the Rules for Responsible Internet Use.

Signed: _____

Print Name: _____

Date: _____

Appendix C

Dear Parents

Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of IT skills, Summerfields Primary School provides supervised access to the Internet.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet Service Provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School and the Council cannot be held responsible for the nature or content of materials accessed through the Internet. The Council will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the Pupil Acceptable Use Policy that we operate at Summerfields. We also have a number of leaflets and web-site addresses from national bodies that explain issues further.

Should you wish to discuss any aspect of Internet use please call in or telephone to arrange an appointment.

Yours sincerely

Head Teacher

✂----------

Permission for Internet Access

Parent/Carer's Permission
I give permission for access to the Internet on the terms set out in the above letter.

Signed: _____ Date: _____

Print Name: _____