Summerside Primary Academy

Computing and Online Safety policy

March 2022

Computing Policy

Aims and objectives
Computing is changing the lives of everyone. Through teaching Computing, we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. Computing skills are a major factor in enabling children to be confident, creative and independent learners.

The aims of Computing at Summerside Primary Academy are to enable children:
• to develop Computing capability in finding, selecting and using information;
• to use Computing for effective and appropriate communication;
• to monitor and control events both real and imaginary;
• to apply hardware and software for creative and appropriate uses of information;
• to apply their Computing skills and knowledge to their learning in other areas;
• to use their Computing skills to develop their language and communication skills;
• to explore their attitudes towards Computing and its value to them and society in general. For example, to learn about issues of security, confidentiality and accuracy.

Teaching and learning style
As the aims of Computing are to equip children with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and as practical as possible. As well as giving children direct instruction on how to use hardware or software in 'skills' lessons, we often use Computing capabilities to support teaching across the curriculum. So, for example, children might research a history topic by using a safe search engine or a website already checked by the teacher. In science/ maths children might use the computer/ iPad to model a problem or to analyse data. We encourage the children to explore ways in which the use of Computing can improve their results, for example, how a piece of writing can be edited or how the presentation of a piece of work can be improved by moving text about etc.

We recognise that all classes have children with differing Computing prior experience and abilities. This is especially true when some children have access to technology at home, while others do not. We provide suitable learning opportunities for all children by matching the challenge of the task to the ability and experience of the child.
We achieve this in a variety of ways, by:
• setting common tasks which are open-ended and can have a variety of responses.
• setting tasks of increasing difficulty (not all children complete all tasks).
• providing resources of different complexity that are matched to the ability of the child.
• using classroom assistants and teachers to support the work of individual children or groups of children.

Computing curriculum planning
The school uses the National Curriculum for Computing as the basis for its curriculum planning. We have adapted this to the local circumstances of the school and the software in place.
We plan our Computing curriculum using a long & medium term plan. The long-term plan maps the Computing topics that the children study in each term. Our medium-term Computing plan shows how teaching units are distributed across the year groups, and how these fit together to ensure progression within the curriculum plan.
The topics studied in Computing are planned to build upon prior learning. There is also an opportunity for teachers to use Computing in other curriculum areas. For example: creating PowerPoint presentations that relate to a period in history.

EYFS

Children have access to the IWB (interactive whiteboard) throughout the day. All staff have an iPad that they use to record their children's progress on Tapestry. An iPad 'station' is set up in our continuous provision to ensure children have access to iPads and are building Computing skills independently. There is a laptop per class that children have access to during the day. Beebots are used when appropriate to the learning indoors and outdoors.

Computing contributes to teaching and learning in all curriculum areas.

English
Through the development of keyboard skills and the use of computers, children learn how to edit and revise text. It can also be used for those who have specific needs relating to writing; offering them an opportunity to type work or use packages that support sentence composition.

Mathematics
Many Computing activities build upon the mathematical skills of the children. Children use coding devices such as BeeBots to learn about position and direction. The children also use smartphones, iPads and computers to access their weekly homework on Mathletics. We have lunchtime Mathletics Clubs in school for children who do not have access to the internet and technology at home so that they are not disadvantaged.

Personal, social and health education (PSHE) and citizenship
Computing makes a contribution to the teaching of PSHE and citizenship as children learn to work together in a collaborative manner. Through the discussion of moral issues related to electronic communication, children develop a view about the use and misuse of Computing, and they also gain a knowledge and understanding of the interdependence of people around the world. E-safety is a key part of our Computing curriculum, regular assemblies are held by the Computing leader and a yearly workshop with parents.

Science
The practical use of Computing and relating it to everyday life is essential. In science we use Computing equipment such as data loggers to record sound, light and temperature. IPads and cameras are also an integral part of science, we are able to record findings and children can then draw conclusions from these images.

Teaching Computing to children with SEN
At our school, we teach Computing to all children, whatever their ability. Computing forms part of our school curriculum policy to provide a broad and balanced education for all children. We provide learning opportunities that are matched to the needs of children with additional learning needs. In some instances the use of Computing has a considerable impact on the quality of work that children produce; it increases their confidence and motivation. When planning work in Computing, we can take into account the targets in the children's Individual Education Plans (IEPs). The use of computers can help children in achieving their targets and progressing in their learning.

Assessment and Recording
Teachers assess children's work in Computing by making informal judgements as they observe them during lessons. Pupils' progress is closely monitored by the class teacher.

The Computing subject leader, **Michael Gardiner**, will keeps of the children's work in an electronic portfolio. This demonstrates the expected level of achievement in Computing for each age group in the school.

Resources
All class teachers have their own desktop. These are networked so we can save on a shared network and print to a range of printers around the school. An interactive whiteboard (SMART) has been installed into all classrooms, including in the nursery.

Every computer in the school is linked to the internet.

Along with the computers, the school has the following:

Hardware

- colour and black and white printers
- scanner
- teacher iPads
- mini iPads
- sound System in hall
- sound field in each classroom

Software

- word processing packages
- painting/drawing software;
- clip art;
- a multimedia programme;
- spreadsheets/database programmes;
- control programmes

Monitoring and review

The monitoring of the standards of the children's work and of the quality of teaching in Computing is the responsibility of the Computing subject leader and the Leadership Team. The Computing subject leader is also responsible for supporting colleagues in the teaching of Computing, for keeping informed about current developments in the subject and for providing a strategic lead and direction for the subject in the school. The Computing subject leader regularly discusses the Computing situation with the headteacher. During the year, the Computing subject leader has specially-allocated time for carrying out the vital task of reviewing samples of the children's work and for visiting classes to observe the teaching of Computing.

Online Safety Policy

Context
In England, schools are subject to an increased level of scrutiny by Ofsted Inspectors during school inspections - following the introduction of the new Framework and the Ofsted Briefing Document on Online Safety **-** http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies

Safeguarding
Summerside Primary Academy is aware of its responsibilities in ensuring that technology usage by all network users is responsible, safe and secure.
There are relevant and comprehensive policies in place which are understood and adhered to by all network users.
Effective and safe use of digital resources
Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of Computing and adopt appropriate practices.

The provisions of the *Children Act 2004*, *Working Together to Safeguard Children and Annex C of Keeping Children Safe in Education (see appendix 1)*[1] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

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
- safe from extremism and radicalisation
- secure, stable and cared for.

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use Computing in its various forms.

It is the duty of Summerside Primary Academy to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to Summerside Primary Academy's physical buildings.
This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The Technologies
Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include, for example:

- The Internet
- E-mail
- Instant messaging e.g. Snapchat, Kik, WhatsApp, often using simple web cams
- Education based apps e.g. Mathletics, Oxford Reading Buddy, Microsoft Teams
- Blogs (an online interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites e.g. Facebook, Twitter, Instagram, LinkedIn,
- Video broadcasting sites e.g. YouTube
- Chat Rooms e.g. Teenchat, HabboHotel, MovieStarPlanet, Tik Tok, Houseparty, Monkey
- Gaming Sites e.g. Club Penguin, Minecraft, Twitch, Discord, Fortnite, Roblox
- Gaming consoles with online gaming e.g. Xbox Live, Playstation Network
- Music download sites e.g. iTunes, Amazon
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Smart TVs

Whole school approach to the safe use in Computing
Creating a safe Computing learning environment includes three main elements at Summerside Primary Academy:

- 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.

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 Summerside Primary Academy. The Headteacher, together with the Computing Subject Leader and SLT Team, ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for Online Safety has been designated to a member of the senior leadership team.

Our school **Online Safety and Computing Leader** is the Michael Gardiner
Our Computing Subject Leader ensures they keep up to date with Online Safety issues and guidance through liaison with the Local Authority Online Safety Officer and through organisations such as NAACE and The Child Exploitation and Online Protection (CEOP)[2]. Summerside Primary Academy's Computing Subject Leader ensures the Head, senior management and Governors are updated as necessary.
Governors need to have an overview and understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments to allow them to review the effectiveness of the policy.
All teachers are responsible for promoting and supporting safe behaviours in their classrooms, ensuring pupils are given clear objectives for Internet use, taught what is acceptable and follow the school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with Summerside Primary Academy's Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- GDPR regulations;
- E-Bullying / Cyberbullying procedures;
- Their role in providing Online Safety education for pupils.

Staff are reminded / updated about Online Safety matters at least once a year; this is a standing item on the Business agenda for September Inset. New staff are given an in-depth session using the policy.

Online Safety is an integral part of the Computing Curriculum. Pupils need to know how to control and minimise online risks and how to report a problem.

Summerside Primary Academy makes every effort to engage with parents over Online Safety matters In addition, the school website features a 'Policies' section in the 'About Us' area, where the Computing and Online Safety Policy can be found and we provide parent training and support sessions when appropriate.

Communication

How is the policy introduced to pupils?

- Instruction in responsible and safe use precedes Internet access.
- Online Safety training is included in the Computing Scheme of Work covering both school and home use.

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks may not be mature; the Online Safety rules need to be explained or discussed.
Online Safety is taught in all year groups, covering age-appropriate issues. Useful Online Safety programmes include:

- Barnet and LGfL Online Safety and e-literacy Framework for EYFS-Y6 (https://www.lgfl.net/online-safety/default.aspx)
- Think U Know (www.thinkuknow.co.uk/)
- Grid Club (www.gridclub.com)
- SWGfL Digital Literacy and Citizenship (www.Digital-literacy.org.uk)
- CEOP (https://ceop.police.uk/)

How is the policy discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies
Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their Computing use in school, they should discuss this with their line manager to avoid any possible misunderstanding.
Computing use is widespread and all staff including administrators, site managers, governors and helpers are included in appropriate awareness raising and training. Induction of new staff includes information about Summerside Primary Academy's Online Safety Policy. There are clear procedures for reporting issues.

How is parents' support enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Summerside Primary Academy can help parents plan appropriate supervised use of the Internet at home.

- Internet issues are handled sensitively, and parents are advised accordingly.

- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet are made available to parents e.g. through updates in the newsletter and on the website.

How are complaints regarding Online Safety handled?

Summerside Primary Academy will take 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 Summerside Primary Academy nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview with class teacher, Phase Leader, Deputy Headteacher or Headteacher;
- informing parents or carers;
- fixed term exclusion;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including work];
- referral to Barnet LA Multi Agency Safeguarding Hub / Police.

Our Computing Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and Barnet LA child protection procedures.

Managing the Internet Safely in School

Summerside Primary Academy:

- Does not allow pupils to use the internet unless they are supervised by an adult
- Maintains the filtered broadband connectivity Wave 9;
- Works to ensure any concerns about the system are communicated to) Wave 9 so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus software *Sophos / other* and network set-up so pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with Wave 9 services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Uses individual log-ins to log-on and access Microsoft Teams
- Ensures that no member of staff ever sends personal data over the Internet other than through the school email or by uploading to One Drive (through which data is secured by log-ins and 'sharing' folders/files with only those concerned). Personal level data should not be taken off-site unless it is on an encrypted device.
- Uses 'safer' search engines with pupils and activates 'safe' search where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure Learning Platform e.g. Microsoft Teams work only shared with classmates/class teacher and webpages not published to the outside world.
- Uses **SENSO** – a Reach2 tool to screen for inappropriate content or internet searches are installed on to every laptop in the school. This is reported directly to the Headteacher and Deputy Headteacher.

Use of the Internet (NB: please see Covid Pandemic School Closure Safeguarding addendum in the Safeguarding Policy for additional measures that apply during periods that school/classes/year groups are closed and pupils are working remotely using Microsoft Teams.

Summerside Primary Academy:

- 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.
- Uses the Wave 9 filtering system, which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff should preview all sites before use [where not previously viewed and cached], including any 'comments sections' [e.g. when accessing YouTube videos], to check for suitability. Alternatively, use sites accessed from managed 'safe' environments such as the Twinkl or White Rose.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs staff and students that they must report any failure of the filtering systems directly to the E-safety/Computing Leader, who reports to Wave 9 where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks social networking sites for specific purposes / Internet Literacy lessons;
- Only uses Microsoft Teams which is managed by School admin for video conferencing activity and has 2 members of staff on video conferencing calls with children;
- Only uses approved or checked webcam sites;

- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes;
- Uses closed / simulated environments for e-mail for pupils;
- Requires all staff and volunteers to sign an Online Safety / acceptable use agreement form annually and keeps 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;
- Ensures the named DSLs have appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other Computing technologies, as part of the Online Safety acceptable use agreement form at the time of their daughter's / son's entry to Summerside Primary Academy;
- 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 – the Police and Barnet LA Multi-Agency Safeguarding Team.

Education and Training

Summerside Primary Academy:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any mate rial that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or DSLs.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive Online Safety education programme throughout all Key Stages, built on the LGfL Online Safety curriculum framework (EYFS-Primary). 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 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 web site / 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 search engines work;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be inappropriate, manipulated and how web content can attract the wrong sort of attention;
    - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;

- 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 that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; online gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general Computing security issues linked to their role and responsibilities;
- Updates staff and/or makes training available to staff on the Online Safety education program;
- Runs a programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on Summerside Primary Academy's website;
    - demonstrations, practical sessions held at school;
    - distribution of 'think u know' for parents materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Managing Email

Summerside Primary Academy:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example admin@summerside.barnet.sch.uk/ y5@summerside.barnet.sch.uk for any communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law, we may contact the police.
- Accounts are managed effectively, with up-to-date account details of users
- Staff members who have left the school are removed from the school email system.
- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make e-mail dangerous. We use filtering software to stop unsuitable mail. Suspected failure of software to filter potential spam, phishing emails or viruses to be reported to the Computing co-ordinator or School Business Manager.

Pupils:

- We only use Microsoft Teams with pupils.
- Pupils are introduced to, and use, Microsoft Teams as part of the Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of communicating online i.e.
    - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive a message or e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening messages and emails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted;

Staff:

- Staff only use Office365 e-mail, OneDrive or Microsoft Teams for confidential information;

- Ensure that e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper;
- Staff sign the appropriate school AUP to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Additional support materials can be found at: www.esafety.lgfl.net

Use of digital images

In Summerside Primary Academy:

- The Headteacher and Deputy Headteacher take editorial responsibility to ensure that the website content is accurate, quality of presentation is maintained and complies with copyright;
- Uploading of information on the public website is restricted to Nadine Lewis, Charlotte Trew, Debora Conte and other members of staff as fits their role.
- Summerside Primary Academy's website complies with Reach2's guidelines for publications.
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address and telephone number. Home information or individual e-mail identities will not be published or given out.
- Photographs published on the web do not have full names attached. Adults have the right to refuse permission to publish their image.
- Uploading of information on the school's network (OneDrive) is shared between different staff members according to their responsibilities.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of Summerside Primary Academy's agreement form when their daughter / son joins Summerside Primary Academy. Parents have the right to refuse/limit permission for their child's image to be published/ Permissions are listed on Arbor Student Profiles under the Consents section and updated by the Office.
- Digital images / videos of pupils are stored in the 'Staff Shared' folders and images should be deleted at the end of the year – unless an item is specifically kept for a key school publication, evidence for professional development or educational purposes within school.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to Summerside Primary Academy website.
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs.
- We do not include names in the school newsletter when images accompany the article. Where names are used (when no images present), only the first name of the child is used. Children featured in newsletter images are checked against the 'permission for photos or images latest update' spreadsheet before submission to ensure we have parental permission to publish as newsletters now are accessible to the world via the website.
- Staff sign Summerside Primary Academy's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- Pupils are only able to publish to their own 'safe' space on Microsoft Teams.
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work.
- Pupils are taught about how images can be abused in their eSafety education programme.

Social networking (other than Summerside Primary Academy's website):

- The school will block/filter access to social networking sites.
- Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs, picture of them with their uniform logo in view etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

- Any teachers' official blogs should be password protected and permission given by the Headteacher prior to publication. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students are advised not to publish specific and detailed private thoughts.
- As a school we are aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
- It is not appropriate for a member of staff to have links with a current pupil via a social networking site.

Managing equipment

To ensure the network is used safely, Summerside Primary Academy:

- Ensures staff read and sign that they have understood Summerside Primary Academy's Online Safety Policy. Following this, they are set-up with email access and can be given an individual Office365 log-in username and password.
- **SENSO** – use of Reach2 tool to screen for inappropriate content or internet searches are installed on to every laptop in the school. This is reported directly to the Headteacher and Deputy Headteacher.
- Pupils log into Microsoft Teams with their own individual log in.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find.
- Makes it clear that no one should log-on as another individual user – if two people log on at the same time this may corrupt personal files and profiles.
- Has set-up the network with a shared work area for each class.
- Requires all staff users to always log off when they have finished working or are leaving the computer unattended.
- Requests that staff and pupils do not switch computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch computers off at the end of the day and projectors when they are not being used e.g. between lessons, over lunch break.
- Has set-up the network so that users cannot download executable files / programs.
- Has blocked access to music download or shopping sites – except those approved for educational purposes.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus software maintained up-to-date and Reach2 provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by Summerside Primary Academy is used solely to support their professional responsibilities. Laptops are marked with serial numbers unique to each item and an 'Inventory' master list is kept to show to whom each school laptop is issued and the responsibility for. This list is kept up-to-date by the ICT Technician. Staff should inform the Computing co-ordinator if they wish to reallocate equipment.
- Makes clear that staff accessing Reach2 systems do so in accordance with any Reach2 policies.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by Site Managers; equipment installed and checked by approved Suppliers/ IT Technician.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.
- Does not allow any outside Agencies to access our network remotely except where there is a need for it e.g. technical support.
- Provides pupils and staff with access to content and resources through the approved Learning Platforms (Office365, OneDrive and Microsoft Teams) which staff and pupils access using their own log in details.

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or sent within the Reach2 approved secure system.
- Follows Reach2 and LGFL advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Reviews the school ICT systems regularly with regard to security.

Electronic Devices – Searching and Deletion

The changing face of information technologies and ever-increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

Please see appendix in our **Behaviour Policy** for more information

Child Pornography

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: **0808 100 00 40**

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/reporting_abuse.html

http://www.iwf.org.uk

How will staff and pupils be informed of these procedures?

- They are fully explained within this policy. All staff will be required to read Summerside Primary Academy's Online Safety Policy acceptance form and to sign indicating that they have read this policy.
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours.
- Summerside Primary Academy's Online Safety policy will be made available on the school website

Role of the SLT

- Developing, owning and promoting the Online Safety vision to all members of Summerside community
- Supporting the development of an Online Safety culture
- Making appropriate resources available to support the development of an Online Safety culture
- Receiving and regularly reviewing Online Safety incident logs
- Supporting the ICT leader in the appropriate escalation of Online Safety incidents
- Taking ultimate responsibility for Online Safety incidents

Role of the ICT leader

- Developing an e-safe culture and acting as a named point of contact for all Online Safety issues
- Promoting Online Safety to all groups of Summerside community
- Ensuring that Online Safety is embedded within CPD for staff and across the curriculum
- Developing an understanding of the relevant legislation

- Liaising with the LA and other agencies as appropriate
- Reviewing and updating Online Safety policies and practice on a regular basis.

Role of the teaching and support staff

- Contributing to the development of Online Safety policies
- Reading and signing staff Acceptable Use Agreements and adhering to them
- Having an awareness of Online Safety issues and how they relate to the children in their care
- Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives
- Embedding Online Safety education in curriculum delivery wherever possible
- Identifying individuals of concern and taking appropriate action
- Knowing when and how to escalate Online Safety issues
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school
- Taking personal responsibility for their professional development in this area

Role of parents and carers

- Contributing to the development of Online Safety policies
- Using the school website and other network resources safely and appropriately
- Discussing Online Safety issues with their children, supporting Summerside in its Online Safety approaches and reinforcing their behaviours at home
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Modelling appropriate uses of new and emerging technologies
- Liaising with Summerside if they suspect, or have identified, that their child is conducting risky behaviour online

Appendices

Appendix 1 – Summerside Acceptable Use Agreement

Staff, Governors and Volunteers (including placement students)

This agreement covers the use of digital technologies across all REAch2 schools including email, internet, shared network drives, network resources, all software, electronic equipment and all systems.

By signing this agreement, you are confirming that:

- I will only use Trust digital technology resources and systems for professional purposes.
- I will not reveal my password(s) to anyone.
- I will follow 'best practice' advice in the creation and use of my password(s). If my password is compromised, I will ensure I change it.
- I will not use anyone else's password, nor seek to discover it. If a colleague does reveal it to me, I will advise them to change it.
- I will not allow unauthorised individuals to access any of REAch2 or school systems.
- I will ensure all documents and digital resources are saved, accessed and deleted in accordance with the Trust network, data security and confidentiality protocols.
- I will not engage in any online activity that compromises my professional responsibilities, school handbook guidance or professional boundaries.
- My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods, even if they have recently left or no longer use the service.
- I will use the approved email system for all email communication related to my work and will not use any personal email accounts.
- I will not browse, download or send material that could be considered offensive to colleagues or others.
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to the Trust Data Protection Officer.
- I will not download any software or resources that may compromise the network, that breach a user's copyright or is not correctly licenced.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop, notebook or other electronic device (including USB flash drive) to the network that does not have up-to-date anti-virus software.
- I will not use a personal digital camera or camera phone for taking and transferring images of children/young people or staff/volunteers without written permission, and if permission is granted, I will use those images only for their intended purpose.
- I will ensure that any personal social networking sites/blogs, Twitter, Instagram accounts etc., that I create or actively contribute to, are separate from my professional role.
- I will follow Trust data security protocols when using confidential data at any location.
- I will access Trust resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those resources.

I understand that:

- It is my responsibility to ensure that my use of social networking sites/blogs, etc., does not compromise my professional role, and I will ensure that my privacy settings are appropriate.
- Any computer, laptop or electronic device loaned to me by the Trust or Academy is provided solely for professional use.
- Any confidential data that I transport from one location to another will be protected by encryption.
- Any information seen by me, linked to service users will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority, e.g. Children's Social Care and/or the police.

- It is my duty to support a whole organisation safeguarding approach and I will alert the schools named designated safeguarding lead /relevant senior member of staff if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern.
- It is my responsibility to ensure that I remain up-to-date, read and understand the online safety policies.
- all internet/network usage can be logged and this information can be made available to my line manager on request.
- failure to comply with any aspect of this agreement could lead to disciplinary action.

I wish to have a network account; an email account; and be connected to all systems that are relevant to my post and I agree to abide by this Acceptable Use Agreement at all times.

Full name:

Academy/Central Team: Summerside Primary Academy
Job title:
Date:
Signature:

Appendix 2 – Senso letter to families

12th February 2021

Dear parents/carers,
We have been very pleased to provide your child with a school laptop to support them with remote learning. We hope they are enjoying using it to complete their lessons and connect with classmates and school staff.
As you are aware, the internet can be brilliant to help children with their learning and presents us with many opportunities that we would not otherwise have. However, we also know that there are some risks when children are online and it is important that children and adults are both aware of these risks to keep them safe.
As part of our safeguarding responsibility for children who are using school devices to access remote learning, a programme called Senso has been installed on your child's device. This allows for remote monitoring of online activity, to make sure that the content that children access on their school laptop is safe. Senso recognises a list of high risk and unsafe words and phrases, and it captures the date, time and a screen shot of what is happening on the device at the time when a word from the alert list has been identified.
Leaders in our school who are responsible for safeguarding children will receive reports from the Senso system with details about any alerts that have been logged for our school devices. This is so that we can respond and put in place any additional support or actions to help children to stay safe.
We will also respond to any alerts that indicate misuse of the device, i.e. not a remote learning activity assigned by the school, and continued misuse of the device may lead to it being returned to the school.
In addition, access to the internet will be remotely disabled on our school devices from 9pm every evening. It will be turned on at 7am. This decision has been taken to promote the health and wellbeing of our pupils, and to support them and you in managing screen time.

Please take this opportunity to discuss the content of this letter with your child so that they are aware of our expectations about how to safely use their school device. Enclosed below are links to sites with useful parent resources to support with online safety.
National Online Safety – online safety guides
O2 and NSPCC Net Aware – online safety advice and guidance

Thank you for your support.
Headteacher