Ashurst Primary School

Computing, Safer Internet & E-Safety Policy

September 2018

Our Computing Policy has been developed based on LA and government guidance. It relates to other policies including Anti-bullying, Positive Behaviour and Child Protection and Safeguarding. It has been agreed by our senior leadership teams, our staff and approved by our **Governors during Autumn term 2018.** The School's Computing, Safer Internet & E-Safety Policy will be reviewed every three years unless updates are required earlier.

Our Vision

Computing is changing the lives of everyone. Through teaching computing skills we equip children to participate in a rapidly- changing world where work and leisure activities are increasingly transformed by technology. Advances in technology will be embraced by all of our learners, including our adult learners, because we are responsible for engaging and motivating our learners to create a cohesive community both in the real and virtual worlds. Computing skills are a major factor in enabling children to be confident, creative and independent life-long learners, ensuring success for 21st Century leaners.

Leadership & Management

Computing is a focus within our School Improvement Plan. Within Ashurst Primary School the Computing leader oversees the strategic planned development within our school. The leader is responsible for moving our school forward and ensuring support is in place to develop staff capabilities in the continually developing field of Computing. Our Computing Leader will attend relevant courses and network meetings to enable them to steer and lead the school's developments with regard to the latest technological advancements.
The Computing Leader will not act as a technician, but will advise colleagues on managing equipment and software and liaise with the onsite technician who visits weekly. The responsibility for the maintenance will fall with the provider of the Service Level Agreement (SLA), currently Agilisys Computer Services. All faults must be reported to Agilisys via the online form. The Computing Leader will ensure that the technicians are contacted to resolve the issues during their regular visits to school. Any decisions with regard to replacements must be agreed by the Senior Leadership Team and Governors.

The Computing Leader is responsible for ensuring effective teaching and coverage of Computing and E-Safety knowledge and skills via the use of Purple Mash. Staff are provided with up to date training and supported by the Computing Leader in sharing expertise and monitoring the quality of provision.

Online Safety

As detailed in 'Keeping Children Safe in Education' (September 2018). *The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalization, sexual predation: technology often provides a platform that facilitates them. An effective approach to online safety empowers school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.*

The breadth of issues classified with online safety is considerable, but can be categorised into three areas of risk:

- ***Content:*** *being exposed to illegal, inappropriate or harmful for example pornography, fake news, racist ot radical and extremist views;*
- ***Contact:*** *being subject to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and*
- ***Conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.*

At Ashurst Primary School we ensure opportunities to teach safeguarding, including online are part of the Computing Curriculum supported by the vigilant culture and values within the school where pupil voice is listened to and support offered in line with Child Protection and Safeguarding Policy, Positive behvaiour Policy and Anti-bullying Policy.

E-Safety & Online Protection

All computers within schools are fitted with a recommended e-safety software package. Apple I-pads/I-pods are filtered through the server. This will allow the Headteacher, Pastoral Manager and Deputy Headteacher as Lead/Deputy designated Child Protection Officers and the SLT to monitor the appropriate use of Computing equipment within schools. All staff, learners and families within our schools are made aware of this software and its usage and all incidents will be dealt with using the appropriate procedures to safeguard children (Please refer to Appendices 1 & 2).
Weekly reports are sent to the Heateacher using Smoothwall which identified any potential breaches and allows further investigation. Any follow up investigation causing concern linking to child safety, peer on peer abuse or Prevent Duty will be dealt with in terms of procedures detailed in linked policies:
Anti-bullying Policy
Child Protection and Safeguarding

Positive Behaviour

Staff will be aware that all users of the school systems must use their personal account because all digital traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.
Learners will be informed that network and Internet use is monitored by e-safety software.
E-safety rules will be posted in all wireless active rooms and discussed with the learners at the start of every year and at regular intervals throughout the year (termly).
All pupils are taught to handle hardware correctly and to access software and the internet safely (Please refer to Appendix 3), as well as due adherence to health and electrical safety when switching computers on and off using the correct procedures.
Parents'/Carers' attention will be drawn to the ICT Policy and e-safety in newsletters, the school prospectus and on the school Website.

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource, along with the LA's Guidance for Schools on Acceptable Use of IT.
- Parents/Carers and learners will be asked to sign and return an Internet Access consent form and an 'Acceptable Use Agreement' with their child(ren). See Appendix 4
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance staff may have temporary access, a member of staff may leave or a pupil's access be withdrawn.
- In our Foundation Stage and Key Stage 1 departments, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials e.g. Education City.
- All staff are expected to search sites prior to using them for teaching and learning ensuring the content is appropriate and safe linking to learning context.

Sanctions for Mis-Use

Any breach of our Acceptable Use Policy will be considered a serious risk to health, safety and security (Please refer to Appendices 2, 4, and 5) and will lead to the following: Access is seen as a privilege, not a right and that access to the Internet requires responsibility.

- An incident review meeting with a member of our school's SLT.
- Temporary or permanent bans on Internet access and learner's parents/carers will be informed.
- All major incidents will be catalogued and reported to our Governors and for the purpose of criminal investigations. The designated/deputy child protection officers will lead investigations and report incidents following procedures detailed in the Child Protection and Safeguarding Policy. These include incidents linked to Peer on Peer Abuse including:
    - Bullying online comments
    - Sexual violence and sexual harassment via online comments/images
    - Sexting
    - Initiation/hazing type of violence and rituals
    - Prevent Duty

- Parents/Carers will be expected to promote safe and secure online activity with their child(ren).
- In the case of employees, any breach may also be considered a breach of the employee's conditions of service which could lead to appropriate disciplinary action including dismissal on grounds of gross misconduct.

1.4 Managing filtering

- The school will work with St Helens LA and the Internet Service Provider to ensure systems to protect learners are regularly reviewed and improved.
- If staff or learners discover an unsuitable site, either when performing internet searches or when accessing links within sites, it must be reported to the e-Safety Leader/Headteacher.
- SLT staff and ICT maintenance staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.5 Managing videoconferencing, I-pad videos & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Alternatively SKYPE permissions can be sought and approved via Agilisys.
- Learners must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the learners' age.
- I-pads will only be used to video learning opportunities as a point of celebration, discussion and reflection to improve performance e.g. drama. At all times an adult will supervise such activity ensuring appropriate use.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and, where necessary, SLT will undertake a risk assessment before use in schools is allowed.
- All mobile phones **will not be used** during lessons or formal school time. The sending of abusive or inappropriate text messages/images is forbidden and will not be tolerated as detailed in the Mobile Phone Policy and in the Child Protection and Safeguarding Policy, Anti-bullying Policy:- referred to as 'Peer on Peer' abuse including sexting, sexual violence and sexual harassment online bullying
- Learners are required to hand in all mobile phones and handheld devices at the start of the school day. They will be securely stored in the school's offices and returned to learners at the close of school.
- Devices that can bypass our school's filtering systems will be carefully monitored by all staff ensuring adult supervision at all times.

Professional Development

One staff meeting every term will be arranged for staff to work on Computing. This will include:

- E-Safety Training provided by CEOP
- Development of Online Learning Spaces
- Introduction to new software/sharing ideas
- General training for Computing procedures
- Whole school support in planning for Computing
- Moderation of children's work for our Computing e-portfolio All staff will attend relevant training, and have opportunities to work alongside other professionals through Peer Coaching sessions within our school. The Computing Leader will also complete on-line e-safety training.

Curriculum

Computing will be integral and used as a tool to enhance all other areas of learning. In addition, we aim to promote the skills and knowledge of Computing as a subject in its own right using Purple Mash. Computing capability will be delivered though the progression of skills based on the National Curriculum age related expectations and objectives. E-Safety will be embedded within the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum using a range of materials suggested on the CEOP website.

E- safety will be continuously delivered as part of the vigilant culture within Ashurst Primary School and ensuring our learners are aware of potential risks when online. This will be further enhanced with annual E-safety Days involving children and parents in designing posters to promote e-safety. Online safety is seen by all as key aspect in ensuring children are keeping themselves safe. By ensuring an open culture in which children feel safe to ask questions and explore their personal experiences, we are able to then support and ensure the necessary procedures are followed in line with Child Protection and Safeguarding Policy linked to 'Keeping Children Safe in Education' September 2018.

Skills and knowledge

Purple Mash resource is used to ensure effective coverage and delivery of the key skills and knowledge. We aim to:

- promote and develop confidence and proficiency in the use of Computing in all learners, including adult learners.
- develop an appreciation and proficiency in the use of Computing in the context of the wider world.
- promote the enrichment of learning, self-led study and collaborative work.
- develop the ability to use Computing appropriately and to choose software suitable for a particular task.
- promote Computing skills through contexts for learning.
- encourage problem solving and investigation.
- ensure that provision for the development of Computing has a strategic focus to ensure future advances

are catered for.
- provide continuity and progression in the strands of the Computing National Curriculum.
- Communication and Handling Information – using Computing to generate and communicate ideas in written, visual or aural forms and to retrieve, analyse and amend information. This will include communication via email and the Internet for research.
- To develop the use of communications beyond the schools (e-mail, video- conferencing and Virtual Learning).
- To develop the use of the Internet as a data/research and communication tool.
- Control and Monitoring – using Computing to control and monitor external events.
- Modelling – to explore computer representations of ideas and of real and imaginary situations.

Teaching and Learning

The Internet is an essential element in the life of our 21st century learners - for education, business and social interaction. The schools have a duty to provide our learners with quality Internet access as part of their everyday learning experiences. The Internet is a part of the statutory curriculum and a necessary tool for staff and learners.

Activities will be planned and targeted according to each learner's individual and different needs, building on their previous learning and skills and giving learners opportunities to apply their skills in different contexts.

Computing will be delivered through a variety of teaching and learning methods e.g. whole class, group and individual work via Purple Mash. Differentiation and progression is ensured by a variety of approaches such as:

- Same activity but different expectations of outcome.
- Same theme, but different levels of input.
- Allowing for different pace of working.
- Different groupings of learners.
- Use of SOS (Share Our Skills) via Kagan teaching and philosophy

Internet use will enhance learning

- Our school Internet access is designed expressly for learner use and will include filtering appropriate to the age of learners.
- Learners will be taught about acceptable and appropriate Internet use and they will be given clear objectives for Internet use.
- Learners will be educated in the effective use of the Internet to support their research, including the skills of knowledge location, retrieval and evaluation.
- Learners will be shown how to publish and present information to a wider audience.

Learners will be taught how to evaluate Internet content

- Learners should not be allowed to use sites such as Google to search for images unless under the direction of the teacher during research sessions. Results of searches **must always be checked by staff prior to classroom use.**
- We will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Learners will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.
- Learners will be taught about responsible online activity and about how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector's World. In addition to reporting any concerns to an adult enabling appropriate action and procedures to be followed.
- Learners are responsible for good behaviour on the Internet just as they are in a classroom or when representing the schools in any way. General school rules apply.
- Outside of school, families bear responsibility for guidance as they must also exercise with information sources such as television, radio, newspapers, magazines, telephones, films and other potentially offensive material. Any concerns that come to light in school about inappropriate access and content being viewed will be discussed with parents/carers and logged on CPOMS safeguarding system. Should any inappropriate content and access affect behaviour then procedures will be adhered to as detailed in the following policies:
  Child Protection and Safeguarding
  Positive Behaviour Policy

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Learners will be advised never to give out personal details of any kind which may identify them or their location.
- Learners and parents/carers will be advised that the use of social network spaces outside school is inappropriate for primary aged learners- see social networking advice attached.
- Staff will adhere to guidelines within the staff code of conduct completed annually.

E-mail

- Learners and staff may only use the designated e-mail accounts on the school systems. All other e-mail accounts are prohibited.
- Learners will immediately inform a member of staff if they receive e-mail that they consider to be offensive. E-mail communication will be taught via Purple Mash.
- Learners will ensure that personal details about themselves or others are not included in any e-mail communication and learners will be taught not to use e-mail to arrange to meet anyone.
- All e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Individual and Different Needs

Our school recognises the advantages of the use of Computing by learners with individual and different needs. Using Computing devices can:

- Address learner's individual needs
- Increase access to the curriculum
- Enhance language skills
- Provide a greater level of challenge for more able learners
- Allow demonstration of their skills and talents

Time Allocation

All classes will have regular access to Computing (Laptops/I-pads/Digi- Blues etc). Further opportunities to develop and extend Computing capability will be provided by the use of laptops to support continuous provision. The latest timetables can be located on the school servers and in the Staffroom.

Equal Opportunities

Our school promotes equal opportunities for computer usage and fairness of distribution of ICT resources. Where learners cannot access ICT at home, school will provide opportunities outside of normal school hours, i.e. lunchtimes or after school.

Resources

The school resources include:

- Calculators
- Computers/Laptops/I-pads
- Access to email and internet
- Scanner
- Digital cameras/WebCams/Camcorder
- Apple I-pods
- Roamers/Beebots/Probots/Lego Mindstorms
- Blog site
- Visualisers
- Purple Mash

Staff will organise their online spaces and resources in such a way that point learners to sites/links which have been reviewed and evaluated prior to use. While learners may be able to move beyond these resources to others which have not been evaluated by staff or recognised providers, learners will be provided with guidelines and lists of age appropriate resources particularly suited to the learning objectives.

All learners will be informed of their rights and responsibilities as electronic resource users before their first use. To enable learners to conduct research and complete their studies and tasks, staff will give regular reminders about acceptable use referring to our e-safety rules, which should be displayed in every room where learners access ICT.

Software

Purple Mash resource is used to deliver the teaching and learning of Computing and E-safety supplemented by other resources. All individuals have access to software that is relevant to them by logging onto our servers. Any software that does not have a site license must only be installed on the individual class laptop only. Our maintenance provider, Agilisys, is responsible for the installation of software onto the school servers.

Network Access Control

In accordance with Agilisys procedures, the ICT technician will have access as necessary to any information and applications systems. Any method of log-on which nullifies the password control is prohibited.

Every user will have an individual username and password. The use of another person's username is strictly prohibited. Passwords must not be printed or displayed on input.

Passwords must be changed immediately if it is suspected that the password has been disclosed. Access rights for all leavers will be removed immediately. Access rights for all users should be reviewed and updated periodically.

Equipment Security Procedures

The Headteacher is responsible for all ICT facilities installed within our school and for ensuring their proper use. The use of ICT facilities not directly concerned with our School's business is prohibited. All items of equipment must be security marked in accordance with the School's risk management policies and included on the inventories. The schools have an alarmed system installed throughout. The Server is stored securely within the building each night. The school's laptops and other Mobile Technology are stored in locked central/classroom cupboards/trolley.

Equipment must only be kept in secure areas, not able to be accessed by members of the public or unsupervised representatives of other organisations. Where equipment is located within central areas and can be accessed by members of the public or in unsecured offices and left unattended for periods of time, the following measures will be considered to deter the theft of that equipment:

- Steel cable attachments locking equipment to the work surface
- Improved security of the outer walls and windows
- Intruder alarm

Laptops must not be left unattended when logged in to applications. If not in use they must be logged out or protected by a secure screen saver. **Users must log out of the systems and the network before signing out of work and also switch off all electrical equipment.**

All the above ensure we comply with new GDPR regulations protecting online data.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Sophos Anti-Virus protection will be updated regularly.
- Security strategies will be discussed in relation to St Helens LA IT Security guidelines.

Portable Resources

The permission of the Headteacher must be received before any loaned equipment leaves the school building. The removal of equipment should be recorded and monitored with records for equipment 'on loan' stored in the main admin Office. Equipment must not be left in unattended vehicles for which insurance is not available and staff will not comply with GDPR regulations. As delivered in GDPR training staff laptops being taken home must be stored in the boot of the car for the immediate journey home and then removed immediately to be stored securely at home address. Thus ensuring GDPR compliance.
All staff laptops to support Teaching and Learning activities will be loaned to members of staff following completion of a signed agreement of long term loan. Unlicensed, illegal or unauthorised software or information must not be installed, used, copied, altered or distributed. Illegal or improper access to external networks, services or facilities is prohibited. ICT equipment on loan to staff will be subject to an annual

hardware check and software update completed by Agilisys.
(Please refer to Appendix 6- Staff Long Term Loan Agreement).

Disposal of Obsolete Resources

The disposal of obsolete computer equipment is governed by The Governors. The Governors should authorise all write offs and disposals of surplus stocks and equipment in accordance with DfE regulations. All information should be physically deleted, corrupted or overwritten so as to make it irrecoverable. Software is not offered to an external agency unless there is a legal right to do so and licence records are adjusted accordingly. Office staff ensure inventories are updated to record the disposal.

Assessment

Assessment for learning will be carried out by teachers in the course of each unit of study via Purple Mash. This assessment may focus on:

- Discussion of the features of the software used.
- The outcomes of work assigned to our learners.
- Strategic questions to monitor understanding of skills and their application.
- Online tasks completed on Purple Mash

Learner attainment is assessed and recorded every term on O'Track assessment best fit. The Computing leader will monitor learners' digital work and compile a portfolio of evidence to celebrate impact. Each year different learners will be selected to participate in pupil voice interviews about their Computing work to ensure consistency and continuity across the school. Feedback will be given to SLT and staff re: peer coaching opportunities and up- levelling learners' work. Evidence of assessed work is stored on Purple Mash resource program. Parents/carers will receive a written comment as part of the annual report sent out at the end of the Summer Term every year.

Definition and Classification of Information

Within this Policy 'information' is defined as data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types regardless of how or where within the School the information is stored or managed.

Information Backup

The Headteacher. Deputy Head and Senior Leadership Team must make sure that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment. All information must be protected by a procedure for archiving and copying for security backup. The procedure must incorporate daily, weekly, monthly, year end cycles appropriate to the type of information, frequency of update, legal and operational requirements. Security back up copies will be stored wherever possible off site from the location at which the operational information is maintained. The ability to restore information from back-up copies must be tested periodically to ensure that procedures, equipment and storage media are performing correctly. Agilisys complete this process on our behalf, ensuring compliance with GDPR.

Compliance with Legal Requirements

All Computing data must be stored and disposed of with due regard to its sensitivity and the requirements of the General Data Protection Regulations May 2018. Personal data will be recorded, processed, transferred and made available according to the new General Data Protection Regulations. See GDPR policy.

Publishing Material Online

Our school website can be accessed by anyone on the Internet. A web page can celebrate good work, promote the schools, reflect recent and future school events, publish resources for homework or projects and highlight other sites worth visiting. Any photos or learners work published will have consent provided in the data collection sheets in line with GDPR May 2018.

Published content on the school websites

The Headteacher and SLT will take overall editorial responsibility, however all staff are responsible for ensuring that content is accurate, up to date and appropriate.

The web page will comply with our schools and the DfE guidelines for publications.
The contact details on our school's websites will be the school addresses, e-mail and telephone number. Staff or learners' personal information will not be published.

Publishing learners' images and work

- Learners will be taught to publish for a wide range of audiences including Governors, parents/carers, prospective parents/carers, past learners or younger learners.
- Photographs that include learners will be selected carefully and will not enable individual learners to be clearly identified.
- Learners' full names will not be used anywhere on the website or Twitter, particularly when attached to photographs.
- Parents/Carers are asked to sign a GDPR Consent Form as part of the Data Collection Sheet which covers use of the Internet on entry to school before photographs/videos of learners are published on the school website or Twitter.
- Learner's work can only be published with the permission of the learner and parents/carers. All material must be the author's own work, credit other work included or accessed and state clearly the author's identity or status.

General

Community use of the Internet

- The school will liaise with local organisations and educational establishments to ensure a common approach to e-safety.
- All temporary users (including staff from other establishments, regular supply staff, parents/carers etc) will be allowed to have access to the school systems using guest individual usernames and passwords.

Assessing risks

- The schools will take all reasonable precautions to ensure that users only access appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Neither the school nor Governors can accept liability for the material accessed, or any consequences of Internet access.
- The schools will audit Computing provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a member of SLT.

Any complaint about staff misuse will be referred to our Headteacher.
Complaints of a child protection nature will be dealt with in accordance with our school's Child Protection and Safeguarding procedures.
Learners and parents/carers will be informed of the complaints procedure and have access via the website.
Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues. This Policy was reviewed with due regard to the Equality Act 2010 and was presented and approved by Governors during the **Autumn Term 2019**.

Signed: _____(Chair of Governors)

Date: _____

Appendix 1- e-safety notification

ASHURST PRIMARY SCHOOL E-SAFETY SOFTWARE

Dear all,

As a result of guidance and as an important part of protecting our children, young people and members of staff, our e-safety forensic software has been installed onto our school Network. All laptops belonging to school, including staff laptops have been connected to this so please be aware of the following points.

All staff and learners must only log on using their own individual username and password when accessing the school system- including e-mail. Please ensure that users log off before leaving their computer unattended for long periods. All access to shared usernames e.g. Y3 are now prohibited.

When accessing the internet – please follow the school ICT, internet and acceptable use policies.

Make your Headteacher or Deputy Headteacher aware of any inappropriate information that is accessed or brought to your attention.

Thank you,

ICT Leader

N.B. If using Google images/YouTube, ensure that live searches are not performed in front of learners – you never know what might appear on the screen. If allowing learners to access this site as a learning tool ensure they are aware of the risks and know the procedures to tell someone if inappropriate information appears.

Appendix 2- Notification of e-safety Incidents to parents/Carers

ASHURST PRIMARY SCHOO

Headteacher: Mrs. Lisa Houghton BA(Hons)QTS NPQH

New Glade Hill, Blackbrook, St. Helens, WA11 9QJ

(01744) 678150 Fax: (01744) 678151 E-mail: ashurst@sthelens.org.uk www.ashurst.st-helens.sch

Date

Dear …….,

Unfortunately, your child has chosen to not follow our school guidelines with respect to acceptable internet use. In particular, they have shown a lack of respect to others by

*making inappropriate internet searches/being involved in cyber bullying incidents/displaying extremist, racist , homophobic, sexist views/using inappropriate language to another child (*delete as appropriate)

We take this breach very seriously.

As a result of this behaviour, your child will not be permitted access to the internet during school time. The incident has been reported to the Chair of Governors and logged. Please discuss the incident with your child and encourage them to make the right choices to promote online safety for everyone. Your child will be expected to request access at the end of the six week period and will be reminded about their future online conduct.

We are working hard to ensure online safety for all our learners, staff and parents/carers and appreciate your support with this matter.

Yours sincerely,

Headteacher **ICT Leader**

Appendix 3 – e-safety rules

E-SAFETY RULES

Keeping everyone safe online.

- I will only use school's ICT systems for school related purposes.
- I will only use my designated e-mail address.
- I will only log on to my own personal and other spaces I have access to e.g. blog site
- I will make sure that all my ICT communications with other learners and adults are responsible including other establishments using the internet, e-mail, video conferencing etc.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidently find anything like this I will immediately inform the teacher.
- I will not write, publish or send anything that could be considered unpleasant nasty or hurtful.
- I will not share my own or anyone else' personal details such as name, phone number or home address.
- I will not arrange to meet someone unless this part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep myself, all other learners, staff and Governors safe.
- I will use CEOP Report Abuse Icon or Hector Protector Icon to report any concerns I have and I will tell my teacher about these concerns.
- I understand that my school uses e-safety software to monitor my use of ICT using the school systems and that my parents/carers will be contacted if a member of school staff is concerned about my e-safety.

S

Stay Safe

Don't give out your personal information to people / places you don't know.

M

Don't Meet Up

Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

A

Accepting Files

Accepting emails, files, pictures or texts from people you don't know can cause problems.

R

Reliable?

Check information before you believe it. Is the person or website telling the truth?

T

Tell Someone

Tell an adult if someone or something makes you feel worried or uncomfortable.

Follow these SMART tips to keep yourself safe online!

Appendix 4: Acceptable Use Agreement – Learners

Date

Pupil Acceptable Use Agreement / e-Safety Rules

Dear Parent/ Carer,

ICT including the internet, email, laptops, digital cameras etc has become an important part of everyday learning in our school. We expect all our learners to be safe and responsible when using any ICT. Please discuss these e-Safety rules with your child. If you have any concerns, please refer to the school website where there are links to other helpful sites with a wealth of information on this subject.

- I will only use school's ICT systems for school related purposes and will give due credit to all sources of materials included in my work.
- I will only use my e-mail address and my own personal space and other spaces I have permission to access to on the Internet.
- I will make sure that I act in a responsible manner when communicating (using the internet, e-Mail, Video conferencing etc.) with other learners and adults, including those from other establishments
- I will not download software, subscribe to any goods/services nor buy or sell using school internet systems.
- I will not deliberately look for, write, publish, save or send anything that could be considered unpleasant or nasty. If I accidentally find anything like this, I will turn my screen/monitor off and tell my teacher immediately.
- I will not write, publish or send anything that could be considered unpleasant, nasty or hurtful.
- I will not share my own or anyone else's personal details such as name, photograph, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep myself, all other learners, staff and Governors safe.

- I understand that the school and the Governors take these matters very seriously and will follow the agreed policy for sanctions.
- I understand that school uses E-safety Software to monitor all use of school ICT systems and that the following sanctions will apply if a member of school staff is concerned about my behaviour as a matter of e-Safety.
- My parent/carer, and when applicable external agencies, will be contacted.
- I may receive a temporary or permanent internet ban.

We have discussed these rules and _____ (child's name) agrees to follow the e- Safety rules and to support the safe use of ICT at Ashurst Primary School.

Parent/carer signature:_____ **Date:**_____

Learner signature: _____ **Date**:_____

Appendix 5: Acceptable Use Agreement – staff

Staff Acceptable Use Agreement / Code of conduct

Staff should ensure all ICT/media use is in line with Teachers' Professional Standards and the Social Media Policy. All members of staff are responsible for explaining the rules and their implementations. All members of staff need to be aware of the possible misuses of online access and their responsibilities towards learners. Ashurst Primary School takes its safeguarding duties with utmost seriousness and will not hesitate to enforce all such procedures and legal steps as may be necessary. The computer system is owned by the school/Local Authority, and may be used by learners to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties, the learners, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and e-mail sent or received.

ICT and the related technologies such as e-mail, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff must sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher/Deputy Head and E-Safety Co-ordinator.

- I will only use the school's email / Internet / Server / Authority Intranet / and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher/Governors.
- I will comply with the ICT system security and not disclose any passwords, provided to me by the school/local authority or other related authorities, to any other person.
- I will ensure that all my electronic communications with learners, parents/carers, colleagues, governors, the community, the Local Authority and the DfE are compatible with my professional role, my contract of employment and all safeguarding legislation, policies and procedures.
- I will only use the designated e-mail and the Local Authority's secure e-mail system(s) for all school and Governor related business and understand that the same professional levels of language and content should be applied as for letters or other media.
- I will ensure that personal data, such as data held on SIMS or the school's servers is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal or use school owned equipment for personal financial gain, political purposes or advertising.
- I will not send material that could be considered offensive, illegal or extremist to learners or colleagues.
- Photographic images and video footage of learners will only be taken using school cameras and used for professional purposes and will only be downloaded onto school controlled documents/websites and will not be distributed outside the school network without the permission of the parent/carer.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies under my safeguarding duties and responsibilities.
- I will report any racist, sexist, homophobic or extremist communications from any person in this organisation to my immediate line manager, who will take appropriate action.
- I understand that the school uses E-safety Software to monitor my use of all ICT using the school systems and I understand that any mis-use of ICT is logged and can be made available, on request, to my Headteacher, Governors and/or for the purpose of criminal investigations. User's Signature: I agree to follow this code of conduct and to support the safe use of ICT throughout the school and understand that violation of the above code of conduct will result in a temporary or permanent ban on Internet use and understand that additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour with the possibility of criminal prosecution if incidents relate to safeguarding/LDO involvement.

Full Name: _____ **Signature:** _____

Approval Date: _____ **Approved by:** _____ **(Headteacher)**

Appendix 6 Long Term Loan Agreement – staff

Agreement of Long Term Loan of Laptops/I-pads/Mobile Technology for Learning & Teaching

Employee Name:

Laptop/i-pad Number:

User Name:

Security Number:

Laptop/I-pad Model:

Laptop/I-pad Serial No:

General:
The above equipment is agreed as a long term loan to the named member of staff whilst in the service of Ashurst Primary School. As part of this agreement the member of staff undertakes to make best endeavours to keep the equipment in good condition and safe. The above equipment must be returned to the school when they leave the school's employment.

The laptop/I-pad/mobile technology is loaned for the sole, exclusive use of the member of staff for professional purposes and they are ultimately responsible for all content/access/usage in accordance with safeguarding legislation, policy and procedures.

The laptop/I-pad/mobile technology MUST be kept in school during the school day and kept secure at all times.

The Headteacher can ask for your laptop/I-pad/mobile technology at any time so that software can be installed/changed in accordance with school policy.

The Headteacher or external auditors may also request your laptop/I-pad/mobile technology at any time in order to monitor usage and ensure compliance with safeguarding policy and legislation.

ICT equipment on loan to staff will be subject to an annual hardware check and software update.

Except with prior explicit written permission from the Headtecaher, resources must not be used for school related commercial purposes or monetary gain.

It is recommended that you change your password on a regular basis. You are prohibited from disclosing your password to any individuals. You must safeguard your user area and its contents, and will be responsible for any misuse. You may not search for, access, copy, or use passwords belonging to other people.

It is your responsibility to ensure that all data on the laptop/I-pad/mobile technology is regularly and adequately backed up in accordance with school policy. Please note that the use of unencrypted USB portable devices is not allowed. Data should not be stored on the desktop area of your laptop.

Additional hardware and software may not be installed on to the laptop/I-pad/mobile technology without the written permission of the Headteacher.

The laptop/I-pad/mobile technology is loaned to the member of staff for professional purposes and as such additional hardware, software and device drivers should only be installed by the Ashurst Primary School ICT Co-ordinator or the school's approved agent in accordance with the appropriate licence.

You should check with your Computing Co-ordinator or the school's approved agent that appropriate anti-virus software has been installed on your laptop/I-pad/mobile technology and that it is regularly updated.

You may not copy any software from the laptop/I-pad/mobile technology to any other machine outside of school's control. Pre-installed software must not be removed or the laptop/I-pad/mobile technology reconfigured in any way.

Insurance:
The laptop/I-pad/mobile technology and associated equipment listed is on the school's asset register and is covered under the school's insurance. This insurance covers the use of the laptop/I-pad/mobile technology at the staff member's home. The insurance does not cover damage/loss in transit between the school and the member of staff's home. The laptop/I-pad/mobile technology must not be left unattended in your vehicle at any time.

GDPR:
Staff must ensure that whilst in transit the laptop/I-pad/mobile technology must not be left unattended in your vehicle at any time. The laptop/I-pad/mobile technology must be stored in the boot of the vehivle whilst in transit to your home address and not on the rear or passenger seat.

Password and usernames must not be shared.
Only you are allowed access when taking the laptop/I-pad/mobile technology home, no other family members must use the device.
No data should be stored on the desktop.
Staff are not allowed use of USB sticks.

Repair and maintenance:
The laptop/I-pad/mobile technology and associated equipment listed will be repaired by the supplier for the warranty period and when the school's normal repair arrangements but the member of staff is responsible for transporting the equipment to and from school for repair.

Care for the equipment:
The member of staff agrees to take all reasonable care of the equipment including carrying out normal software or hardware maintenance activities, such as cleaning the equipment, monitoring faults and errors, reporting errors in writing as soon as possible to the designated member of staff.

Acceptable Use:
IT IS NOT ACCEPTABLE to use a school computer/laptop/I-pad/mobile technology for any of the following whether at home or on school premises.

- Accessing, displaying, downloading or printing of any offensive, obscene, pornographic or indecent images, data or other media files.
- Accessing social networking, file sharing and similar sites.
- Accessing gambling or adult only sites.
- Participating in chain letters or registering in chat rooms.
- Posting information that may disparage, harass or cause offence to others on the basis of gender, race, age, disability, religion, sexual orientation, political affiliation, national origin or extremism.
- Publishing statements that are defamatory or information that is false or misleading concerning the school, Governors or any of its customers or business associates.
- Publishing confidential or proprietary information of the school on unsecured Internet sites such as bulletin boards or disseminating such information that might compromise its confidentiality.
- Downloading, using or distributing software, films or executable programs from the internet.
- The transmission or downloading of anything other than copyright free material, including media files.
- Initiating contact with a child for purposes other than curriculum content.
- Use of the internet in any way which brings the school into disrepute.

In addition to the above, staff should also note the following:-
- Your laptop computer/I-pad/mobile technology must only be used for school related professional activity. It is not for personal use and must not be used by anyone else including family members or learners.
- Files containing personal data relating to staff or learners should not be held on the hard disk of your laptop or other portable computer. Where this is impractical then encryption, which renders the data unreadable without the decryption key, should be installed by the Computing Co-ordinator or the school's approved agent. A note of the encryption password must be kept securely in school.
- You may not access or copy directories, programs, files, data or documents which do not belong to you unless you have prior permission from the owner.
- Learners' work that is required for moderation and similar purposes must not be held exclusively on your laptop or other portable computer. The originals or copies must be held on the school's teacher network.
- If your laptop/I-pad/mobile technology is lost or stolen you must inform the Headteacher immediately.

Agreement of Parties:
The school agrees to the long term loan of the equipment to the named member of staff.

ICT Co-ordinator's Signature: _____Date: _____

Headteacher's Signature: _____Date: _____

I acknowledge that I have read and understood the above terms and conditions under which the laptop/I-pad/mobile technology (above) has been loaned to me.

I accept that a breach of the Acceptable Use of this equipment may lead to disciplinary action, up to and including dismissal with the possibility of criminal prosecution if incidents relate to safeguarding/LDO involvement.

I also accept that a charge may be levied against me if I do not comply with this policy and, as a consequence, repairs need to be made to the laptop/I-pad/mobile technology.

Member of staff's Signature: _____ Date: _____

Appendix 7: Data Protection Consent Form – Parents/Carers

Information Sharing at Ashurst Primary School **Ashurst Privacy Notice details how we process and share information.** **This information is available on the school website and a hard copy can be requested at the school office.** **Below are a list of agencies that work with school and request information or process data as part of their service.**	
Music Service – names and dates of birth for certificates	Consent required:
Swimming – names and dates of birth for certificates	Consent required:
I give permission for my child's photograph and/or first name to be taken for school use in publicity and at school events.	Consent required:
I give permission for my child's photo to be taken and used by outside agencies for publicity use (e.g. Saints)	Consent required:
I give permission for my child's photograph and or first name to be used on Twitter	Consent required:
I give permission for my child's photograph and or first name to be used on the school website and school newsletter	Consent required:
I give permission for my child to be videoed in performances e.g. Christmas performance	Consent required:
The agencies below are who we share data with and do not require consent:	
• Ofsted	
• Local authority	
• Social care personnel, where relevant	
• The Department for Education (DfE)	
• Sims- pupil data/ attendance/ assessment	
• School nurse service NHS	
The agencies below are who we share data with:	
• Schools that the pupils attend after leaving us	
• Residential providers	
• Sports coach or other out of school club providers	
• Staff associated with school trips and competitions	
• Other relevant health professionals	
• Third party parent communication providers e.g. Teacher to Parents texting services	
• Catering services Parental Pay System – school meals	
• Assessment providers – O'Track Assessment	
• Inventry – Attendance system	
• Nessy – intervention program	
• 1st Class at Writing – intervention	
• My Book Blog- Reading programme	
• IXL – Maths resource	
• Spag.com – English support online program	
• Micro Librarian system	
• CPOMS – Safeguarding system	
• Tapestry – Early Years assessment program	
• Photograph companies– data held for 12 months and the destroyed securely	
• Music Service – Wider Opportunities	
• Swimming Baths- Swimming lessons/certificates	
GDPR Regulations: **By signing below, I understand that I am giving consent for my child to participate in and access the activities detailed above to support their learning in school. I understand that I can withdraw consent at any point and it is my responsibility to update the school in writing.** **Signed: _____ (Parent/Carer) Date:_____**	