E-SAFETY POLICY

Approved by:	**GB**	**Date:** 04/07/19
Last reviewed on:	July 2019	
Next review due by:	July 2020	

This policy should be read in conjunction with the following policies:

- ***Safeguarding Policy***
- ***Behaviour Policy (Primary & Secondary School)***
- ***Anti-Bullying Policy***
- ***CCTV Policy***
- ***Social Media Policy***
- ***Use of Electronic Devices Policy***
- ***General Data Protection Regulation (GDPR) Policy***
- ***Concerns and Complaints Policy***
- ***Staff Code of Conduct Policy***

1. Policy Overview

Introduction

ICT at The Duston School is an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. We understands that as technology advances new benefits and risks are formed and that we will need to adapt to these. This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimize risks and how to deal with any infringements.

The below must be considered

- E-Safety is a **child protection issue not an ICT issue**. All people working in a school, whether adult or child have a duty to be aware of e-safety at all times, to know the required procedures and to act on them. Please read the schools relevant 'Acceptable use policy'.
- E-safety is not limited to school premises, school equipment or the school day. Neither is it limited to equipment owned by the school. E-safety is a partnership concern. (An incident occurring outside the school and brought to the schools attention will be treated as if it had happened on school premises in the teaching day)

ICT Acceptable Use Agreement

- Staff and Students sign an ICT Acceptable Use Agreement when they join the school (see Appendix 1).

Policy Objective

The latest e-safety guidance states that the breadth of e-safety issues can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

The purpose of this policy is to ensure that the school community are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this as well as the rules and restrictions around the use of ICT and other technology at The Duston School.

Scope

This policy applies to all members of the school community (including staff, students, governors, Parents/carers and any visitors accessing the internet or using technological devices on the school premises and outside. This must include staff or pupil personal devices such as mobile phones and tablets which have been brought onto school grounds. The policy must also take into consideration devices the school has issued members of staff and pupils to use on and off site.

At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and beyond the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and must read and sign the ICT AUP. At The Duston School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school. The Principal ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for E-Safety is detailed below:

- The Principal has overall responsibility for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for e-safety is delegated to a member of SLT.
- A designated member of SLT has responsibility for all child safety and therefore e-safety matters.

- A designated member of SLT along with the IT Systems Manager has accountability for this policy and responsibility to review and update its contents. This will then be agreed and signed off by the Principal and School Governors.
- Teachers and support staff must ensure that they are aware of e-safety issues, policy and practices and that they have understood and abide by the rules outlined in this policy.
- Students are also responsible for using ICT as outlined in this policy.
- Parents/Carers have responsibility for ensuring that they read and understand the terms of this agreement.
- Parents/Carers, volunteers and community users who work on school systems will also be expected to read and abide by the terms set out in this policy.
- Technical support - The ICT Support team is responsible for ensuring that school infrastructure is secure, and not open to misuse or attack. They ensure that the school meets the requirements of this policy. Users can only access the school's network through an enforced password protection policy, in which passwords are regularly changed. Technical support staff inform the IT Systems Manager about any filtering issues, and modify filtering rules as appropriate.
- A designated member of SLT has accountability for data protection and there is a separate data protection (GDPR) policy.

The Duston School believes that it is essential for Parents/Carers to be fully involved with promoting online safety both in and outside of school. We consult and discuss online safety matters with parents, pupils and staff in order to promote a wide understanding of the benefits and risks related to internet usage and ensure we have relevant E-Safety information stands at any curriculum events held.

Education of Pupils and the Curriculum

The most important aspect of keeping young people safe online is education. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience, and to ensure that they are not at risk when they are outside of the safe environment provided at school.

- We have an age-related e-safety curriculum that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, how to take responsibility for their own and others safety and how to be responsible users of technology.
- Key e-safety messages are reinforced through assemblies.
- Acceptable use of the school's ICT systems is discussed with pupils in every class and all classes discuss their rules for e-safety which are displayed in classrooms, student planners and in all computer suites.
- Students are given age appropriate support to search safely and to evaluate the content that they access online. Processes are in place for dealing with any unsuitable material that is found in internet searches. Staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.

- Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Our behaviour policy is also used to reinforce online behaviour with appropriate sanctions for irresponsible use.
- Staff share with pupils how to deal with issues outside school where there may be no filtering
- Teachers monitor ICT use during lessons, including the use of Impero, to monitor student screens.

Parents/Carers

Parents and Carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use guidance
- Letters home with E-Safety information
- Providing E-Safety awareness at school curriculum events

2. Managing Information Systems

The school is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of school data and personal protection of the school community seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. A firewall called Sonicwall, monitors, and protects the network and connection to the internet. The school use's Lightspeed to provide filtering to ensure the online safety of all users. The Anti-Virus and Malware protection software is Microsoft Endpoint Protection.

We regularly

- Update firewall and switch firmware
- Update filtering System
- Update Anti-Virus protection and repositories
- Patch all Systems
- Review Security strategies

The Internet

All staff and students have access to the Internet. It must be used responsibly. Student access to the internet is granted for educational purposes only. Staff access is also granted for use within the remit of their roles at the school. Personal use of the internet is permitted outside of lesson time for students or teaching time for teachers, provided that it does not interfere with the expectations of student and staff duties towards the School and does not contravene any of the terms for acceptable usage outlined in this policy. All users must observe copyright of materials from electronic resources.

Users must not

- Use the Internet for financial gain, gambling or advertising.
- Attempt to access information that is offensive to others.
- Download files including music or video clips that are not related to your work at the School.
- Download any executable files, without consulting the ICT services department.
- View or download offensive, obscene or inappropriate material from any source.
- Use the Internet to order items on behalf of the School or otherwise contractually commit the School without the correct authority
- Copy or distribute school software or illegal software from other sources.

It is at the Principals' discretion as to what internet activities are permissible for staff and pupils and how this is disseminated

Filtering

All Internet access within school is filtered, limiting access to inappropriate content. Different levels of filtering are provided for different age groups of student, and more relaxed rules are also provided for staff. In fulfilling their roles, at times, some colleagues are required to access content which could be deemed as questionable. In such circumstances, staff must advise either their line manager, or the IT Systems Manager before accessing the content. Staff using school devices outside of school must be aware filtering will not be in place, but should not use school owned devices to access anything that could be deemed inappropriate.

As part of the school's responsibilities under the prevent duty, the rules employed by the school's Internet filtering solution are designed to limit potential access to content and sites that could pose a risk to students regarding extremism and radicalisation.

Any changes to the Internet filtering are requested and logged via the ICT Support team, who complete periodic checks of the Internet filtering logs.

Email

All staff and students are provided with a school email account. Email contact between staff and students must be via the school email systems and not via personal email accounts. Users must not use email in any way that could be harmful or distressing to others. All messages should be polite and responsible. Emails must not include anything that is not appropriate to be published generally.

Users must not attempt to hide their name or attempt to send email from another user's account.

Staff are expected to check their email every day, and should configure their automatic Out of Office assistant to reply to emails in any circumstances during the school term when colleagues or parents cannot expect to receive a reply within this set time period.

Please be aware that emails are submissible as evidence in court proceedings and even if deleted can be recovered for use.

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and to ensure school information/data stays on school systems.
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
- All pupils have their own individual school issued accounts and Email.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- The forwarding of viral chain emails is not permitted in school. However the school has set up a support account, itservices@thedustonschool.org, to allow pupils to forward any chain emails causing them anxiety. No action will be taken with this account by any member of the school community
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.
- Staff must follow the incident reporting process if they receive an offensive e-mail.
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware); all the school e-mail policies apply.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.
- Sensitive data emails:
    - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
    - Verify the details, including accurate e-mail address, of any intended recipient of the information.
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

Monitoring

All access and use of the school's systems is logged and screen monitoring software is used. Student emails are also screened for anything that could be deemed inappropriate, including unsuitable language or content that could be seen as cyberbullying.

Logs of every page printed are also kept and any user found printing excessive amounts not related to school, will be charged for the costs of the printing.

Authorised ICT staff and relevant SLT members may:

- Inspect any ICT equipment owned or leased by the school at any time without prior notice. a. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department.
- Monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or visitors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.
- Without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
- Review, record and issue CCTV footage of the activity in the corridors of the school.
- Monitor and review internet activity from an end user account or devices
- The school uses management control tools for controlling and monitoring workstations.

Prior to undertaking any form of investigation that requires accessing a member of staff's files or email account, a privacy impact assessment is always carried out. This helps the school identify if such an investigation is appropriate and assesses any alternative methods of achieving the same aim.

Any investigation which identifies misuse or failure to comply with school rules or policies may result in disciplinary proceedings.

Data Encryption, Data Security and Data Storage

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff and Students are permitted and encouraged to store or save their data onto the School's secure central server.
- Staff laptops which have offline files enabled will have an encrypted hard drive.
- Where possible portable storage devices such as USB data sticks will be encrypted before use with individual passwords. Users are encouraged however not to store any sensitive or personal data on any portable devices.

- All users must take all sensible measures to protect information including but not limited to the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device). This is enforced if School emails are accessible on personal devices.

- Users should also ensure their device auto-locks if inactive for a period of time. The School reserves the right to remotely wipe School email stored on a device in the event of loss or theft.

- If a handheld device cannot be encrypted it must not be used and will not be permitted by the School to store person identifiable data or School emails. Furthermore it must not be connected to any of the School systems, whether by physical (e.g. USB) or wireless connection (e.g. Wi-Fi). The School aims to replace any devices which cannot be encrypted and which are capable of storing personal data where it is possible to do so.

Disposal of Redundant ICT equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the items including an acceptance of responsibility for the destruction of any data.
- All redundant ICT equipment that may have held school data will be physically destroyed with a certificate issued. This is carried out via a WEE certified agency.

3. General Network User

User Accounts and Passwords

All users of the School's ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. The youngest children in the infant school do use shared logons. All passwords must meet the schools complexity requirements, and are forced to be changed regularly.

Users must not share their logon details with others or attempt to log on using another user's account.

Before leaving a computer, all users must ensure it is either locked or you have logged out, ensuring nobody else can access your logon. All users are responsible for any activity that takes place under their user account.

If you aware of a breach of security with your password or account then inform IT Support immediately.

Software Use and Installation

Staff and Students are provided with the software that they require and are not to attempt to add or remove any software to any shared computers without the prior authorisation of a member of the ICT Support team. This includes programs downloaded from the Internet and software brought into school on CD/DVDs/USB keys or via any other means.

In the case of school issued iPads, Apps are administered through the school's mobile device management system. Any required Apps must be requested through the IT Support team.

School Issued Mobile Computing Devices

Many staff and students at The Duston School are issued mobile computing devices, be that laptops or tablet computers, for their individual use. Their use is intended to either support a Student's learning or a member of staff's job role. In the case of these individual use devices, some personal use is allowed as long as it does not interfere with its intended use.

All users are expected to treat any property that belongs to the school with respect and reasonable care. Any faults or breakages must be reported to the ICT services department immediately.

Staff and Students are responsible for the safe keeping of any portable device that has been issued to them and as such they must

- Never leave a School portable computer unattended in an unlocked room, unless it is secured is a locked locker or draw
- Never leave a School portable computer unattended in public places, even for a few seconds.

For the reason of personal safety staff and students are advised not to use school issued mobile computing devices, particularly iPads, on public transport or in other public places. Any such use is at the risk of the member of staff or student.
All school-issued portable devices are insured. However, if a portable computer should be lost or damaged through user negligence, by accepting the device, users acknowledge that they will be liable for the cost of repair or replacement.

Personal Mobile Technologies

Primary and Secondary school students are forbidden to use personal mobile devices in school.

For all other users, Staff, Sixth form students, Governors and visitors; Personal devices are to be used in designated areas. These users have access to the school 'BYOD' and 'Guest' wireless networks, which they can only use once authenticated.

These wireless networks are both fully filtered, tracked and monitored for safeguarding purposes.

Social Media

The school is committed to teaching the responsible use of social media.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of cyber bullying to the school.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored. You can check age restrictions and information on social media apps by clicking here: https://www.net-aware.org.uk/networks/?order=title
- For some parental and community engagement activities, the school has its own official and internally monitored accounts on the social media platforms.

4. Reporting and Dealing with Incidents

Breaches

A breach or suspected breach of policy by a school employee, pupil or visitor may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Staff must report incidents or concerns and the actions taken to the Designated Child Protection CoOrdinator using the appropriate channels, this may include following the Child Protection and/or Safeguarding Procedures.

Where there are concerns about illegal activity the school will report the incident to the Police or Children's Safeguarding Team. If the school is unsure how to proceed with an incident or requires assistance the Northampton County Council e-Safety Officer will be contacted.

Incident reporting

In the event of suspicion, all steps in this procedure should be followed

- Have more than one senior member of staff/volunteer involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer (housed in IT services) that will not be used by young people and if necessary can be taken off site by the police should the need arise. Ideally use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also the sites and content visited are closely monitored and recorded this will provide further protection.
- Make sure you record the URL of any site containing the alleged misuse and describe the nature of the content causing you concern. If possible record and store screen shots of the machine were the incident has taken place. The information collated should be printed out, signed and dated.
- One this has been completed and fully investigated the safeguarding team and e-safety team or lead will need to judge whether the concern has substance or not. If it does then appropriate action will be required and could include the following:
    - PCSO/Police referral
    - Referral to the MASH team (When there are child protection concerns)
    - CEOP
    - CSE toolkit – To look at the risk of CSE

- If there are any concerns around on line grooming this includes images of child abuse the Police should be contacted immediately.

Other circumstances when e-safety concerns should be reported to the Police one discussed with the designated safeguarding officer are highlighted below:

- Radicalisation
- Online Grooming
- Hacking
- Hate Crimes
- Harassment
- Certain types of adult material
- Other criminal conduct, activity or materials

Appendixes

Appendix 1

Acceptable Use Policies (AUP) Student

ICT including the use of the Internet, VLE, email and mobile technologies is an important part of learning at The Duston School. We expect all pupils to be safe and responsible when using any ICT. It is essential that Pupils are aware of safety and know how to stay safe when using ICT. This policy applies to all school computers and devices along with any personal mobile and tablet devices that you bring to use at school.

For my own personal safety:

- I will only use the school's ICT systems, including the internet, e-mail, digital video, and mobile technologies for educational purposes.
- I will not download or install software on school devices. Downloading executable files (.exe) is forbidden
- I will only log on to the school network/VLE with my own username and password. I will keep my password secure and ensure it is changed on a regular basis
- I will not attempt to log on using another person's username and password with or without their permission.
- I will only use my school email address for school communications and will use it in a responsible and sensible manner.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidently come across any such material then I will report it to a member of staff immediately.
- I understand that the school will monitor my use of the ICT systems, email and other digital communications and this info can be made available to my teachers and Parents/Carers.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone external to the school community unless this is approved by my teacher.
- I am aware that when I take images of pupils and/or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school.
- I will not disclose or share personal information about myself or others when on-line.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will not attempt to bypass the internet filtering system.
- I will respect the privacy and ownership of others' work on-line at all times
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.
- I understand that mobile phones and smart watches are not permitted at the Duston School.
- I will only use my personal devices (Laptop/tablet) in school if I have permission and have signed the BYOD Acceptable Use Policy. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Dear Parent/ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the school **safeguarding officer.**

Please return the bottom section of this form which will be kept on record at the school

✂----------

Parent/ carer signature

We have discussed this document with……..(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at The Duston School.

Parent/ Carer Signature ……..…….

Pupil Signature……..

Class …….. Date ……

Appendix 2

Acceptable Use Policy Staff, Governors & Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices 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 are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the safeguarding officer.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes / educational purposes.
- I will keep my password secure and ensure it is changed on a regular basis. I will not disclose this information to anybody.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will ensure that all electronic communications with pupils and staff are for educational / professional purposes only
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will ensure that personal data (such as data held on SIMS or financial software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick.
- I will not install any hardware or software without permission of IT services.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or The Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, SLT or the Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm. Exceptions being in offices and the staff rooms.
- Staff employed by the school should not accept students as friends past or present on social media accounts.
- Staff posting inappropriate comments and media on social media could lead to disciplinary action and having their employment terminated.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted
- I understand this forms part of the terms and conditions of my employment.

Staff Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……..(printed)

Job title ……

Appendix 3

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Parent Info

Parent Info is a new free service for schools. Here you'll find a collection of articles, tips, expert advice and resources designed to help parents keep up with what their children are doing on-line.

Parent Info is a collaboration between The Parent Zone, which has been providing information and support to parents for a decade, and CEOP, the Child Exploitation and Online Protection command of the National Crime Agency.