Our vision:

Achievement for All

Our mission:

To fulfil this through developing every child’s personality, abilities and talents to the full, to be the best they can be.

Philosophy

At Sandgate School**,** we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom through our (LUNS) filtered web access. Pupils and staff are given the support, through advocacy of good practice, to use IT safely. All pupils have their use monitored as appropriate.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Effective safeguarding requires that **everyone** in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties, including staff not directly involved in data handling, who should be made aware of the risks and threats and how to minimise them.

This policy is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, I-pads, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised staff.

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them

Never interfere with any anti-virus software installed on school ICT equipment that you use

If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Breaches

A breach or suspected breach of policy by a Sandgate employee, contractor or pupil may result in the temporary or permanent withdrawal of Sandgate ICT hardware, software or services from the offending individual. The Headteacher may decide to take further action as appropriate.

Incident Reporting

Any security breaches, or attempts, virus notifications, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or E-Safety Co-ordinator.

Data Security

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

Security

- The School gives relevant staff access to its IT System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data and have read the E-

Safety Policy and attended whole school e-safety training.

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. Anyone expecting a confidential/sensitive fax should have warned the sender to notify before it is sent.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency, and recorded in the schools equipment log as appropriately redundant.

No ICT equipment should be disposed of without the prior consent of a member of the school's SLT.

Hard discs and other data recording components should be wiped clean or destroyed prior to disposal.

E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

Managing e-Mail

The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimize the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

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

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

Staff must inform (the E-Safety co-ordinator/ line manager) if they receive an offensive e-mail

Pupils are introduced to e-mail as part of the ICT Scheme of Work if appropriate.

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

The use of Hotmail, BT Internet, Yahoo or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted.

Sending e-Mails

Use your own school e-mail account so that you are clearly identified as the originator of a message

School e-mail is not to be used for personal business of any kind.

Receiving e-Mails

Check your e-mail regularly

Never open attachments unless from a trusted source; Consult your network manager first.

Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

Try to use other, more secure methods.

E-Safety In the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- Educating pupils on the dangers of technologies that maybe encountered outside school is done formally and informally when opportunities arise and as part of the E-Safety curriculum.

Older pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or The Child Exploitation and Online Protection Centre (CEOP) report abuse button.

The Prevent Duty

We are aware through our Prevent training that some young people with learning difficulties have become vulnerable to on-line grooming which encourages their involvement with terrorist groups or activities. We understand that, as part of the Prevent Duty, we must ensure our young people are aware of this risk. It is also part of our policy that if any of our young people are known to spend long hours on the Internet at home, or play unsuitable games, this is noted on a Child Welfare and Safety Concern log, with further liaison with parents and possibly others, taking place.

E-Safety Skills Development for Staff

All staff attend an e-safety course.
All staff must incorporate e-Safety activities and awareness within their curriculum areas.

The ICT subject leader is CEOP trained and is available to provide extra advice to staff, as well as providing regular updates through staff training sessions.

Use of the internet

It is recommended that

- Pupils are supervised when on the internet, unless permission is given by headteacher.
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the headteacher.
Sandgate School E-Safety Incident Log
Details of ALL E-Safety incidents to be recorded by the E-Safety Coordinator.

This incident log will be monitored termly by the Headteacher.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Managing Other Web 2 Technologies

At present, across both school sites access to social networking sites is denied to pupils within school unless supervised through the machine in the sensory room.

Staff are reminded that their duty of confidentiality applies to use of the internet and as such applies to sites such as Facebook etc. School business should not be conducted via such sites and you should not link to parents, carers or students through them.

Skype will only be available through staff accounts and its use will be supervised at all times. School accounts should not be used out of school and the passwords should be kept secure by the class staff.

Youtube may be accessed and downloaded by staff.. Any clips must be viewed in total before being used in a lesson.

Pupils are always reminded to avoid giving out personal details on such sites 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 profiles on such sites to maximum privacy and deny access to unknown individuals

Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

Our pupils are asked to report any incidents of bullying to the school

Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the VLE or other systems approved by the Headteacher.

Parental Involvement

Parents are encouraged to support good practice and share responsibility in safe ICT practice both at home and at school.

Parents are offered training in E-safety Issues at least once a year. Information is also available on the Learning Zone and the school website.

Passwords

Always use your own personal passwords to access computer based services

Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

Staff should change temporary passwords at first logon

It is recommended that passwords are changed termly and are at least 8 characters ; a mixture of upper and lower case letters and some numbers.

Do not record passwords or encryption keys on paper or in an unprotected file

Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

User ID and passwords for staff and pupils who have left the School will be removed by the technician.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Remote Access

You are responsible for all activity via your remote access facility following the procedures outlined in this document.

School ICT Equipment

As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you. Any device provided by school is for the sole use of the staff member and should not be used by any other party.

Ensure that all ICT equipment that you use is kept physically secure.

It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.

Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

A time locking screensaver should be applied to all staff machines. Staff using school computers should log off if they leave the computer.

Privately owned ICT equipment may only be used for school purposes on a school network after consultation with the ICT Subject Leader.

On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

Mobile Technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Servers

The school technician will keep the school server secure and be responsible for backing up the system regularly.

Safe Use of Images

Taking of Images

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils only with school equipment.
- All such images should be stored only on the school network.

Other Info

Read in conjunction with the Anti-Bullying, Behaviour, Data Protection Guidelines and Safeguarding Policies.

Writing and Reviewing this Policy

Staff to be involved in making the Policy for ICT Acceptable Use through SLT.

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

This policy has been read, amended and approved by the staff, head teacher and governors

Primary Pupil Acceptable Use Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, 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 me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

Please turn over, sign and return to school

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page to the office. If you have any concerns or would like some explanation please contact their class teacher or the E-Safety Co-ordinator Colin Pearson.

- - ✂ -

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

Parent/ Carer Signature ……..…………………..……………………………….

Class …………………………………. Date ………………………………

Author	Colin Pearson
Date written	February 2016
Date approved at Governing body	March 2016
Date for review	February 2019 (or sooner if required)

Acceptable Use Agreement: Pupils – Secondary

Secondary Pupil Acceptable Use - Agreement / E-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged
- 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.

Please turn over, sign and return to school

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies 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 E-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the Sandgate School E-Safety coordinator, Colin Pearson.

Please return the bottom section of this form to school for filing.

- -✂- -

Pupil and Parent/ carer signature

We have discussed this document and ……………………………………..........(pupil name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Sandgate School.

Parent/ Carer Signature …….……………………..……………………………….

Pupil Signature…………………………………………………………………….

Form ………………………………… Date ………………………………

Acceptable Use Agreement: Staff, Governors

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Sandgate School E-Safety coordinator or the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.

- I will ensure that personal data (such as data held on MIS 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 authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of Colin Pearson.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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 or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role 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.

User 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………………………………….

Please return completed slips to the office or Colin Pearson (E Safety Coordinator)