E-Safety

Policy

Agreed: September 2019

Date for Review: September 2020

Links To Our Mission Statement and Aims

At Churchtown Primary School our values and vision form the basis of all our policies and practice.The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Churchtown Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff at Churchtown Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for education, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying, which are cross-referenced with other school policies.
- Ensure all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Areas of Risk

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identify theft (including frape (hacking social media profiles)) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well being (amount of time spent online).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film)

(Ref Ofsted 2013)

Scope

The policy applies to all members of Churchtown Primary School community (including staff, students, volunteers, parents/carers visitors, community users) who have access to and are users of school/ academy computer and communication systems, both in and out of Churchtown Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school/academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role and Responsibilities

Leadership Team

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Leadership Team are responsible for ensuring that the ICT Team and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Leadership team should be trained in e-safety issues and be aware of the potential child protection issues.
- The leadership team will liaise with school ICT technical staff and receive reports of e-safety incidents and will log this information and use it to inform future e-safety developments.

Computing/E-Safety Subject Leaders

As part of their role, the Computing Subjects Leaders will take day to day responsibility for e-safety issues and having a leading role in establishing and reviewing e-safety policies/ documents. In addition, they will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- promote an awareness and commitment to e-safeguarding.
- ensure that e-safety education is embedded across the curriculum.
- provide training and advice for staff and parents.
- liaise with the Local Authority and Computing CORE network group.
- liaise with school ICT technical staff and receive reports of e-safety incidents. They will log this information and use it to inform future e-safety developments.
- record and review all incidents relating to extremism in order to establish whether there are any patterns of extremist groups targeting the school and whether current procedures are robust enough to deal with the issue.

Infrastructure Manager / Technical Staff

The Infrastructure Manager is responsible for ensuring that:

- reasonable systems are put in place to ensure that the network and related infrastructure is as secure as possible.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- he keeps up to date with e-safety technical information in order to effectively carry out his e-safety role and to inform and update others as relevant.
- equipment is protected adequately against threats such as hacking and viruses.
- the network infrastructure is monitored regularly and consistently.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (See Appendix 1)

- they report any suspected misuse or problem to the Headteacher / Principal / Senior Leader ; E-Safety Coordinator / Officer (insert others as relevant) for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- e-mails sent to parents/guardians or any other agencies should be on a professional level and sent through office@churchtown.org.uk
- they are aware of those students who may be targeted or exposed to harmful influences from violent extremists via the internet. Students and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies. All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.

Governors

To enable the Governing Body to carry out its duties in promoting high standards of education and achievement, governors need to be fully informed about the standards in E-Safety as well as priorities for development. Governors are kept informed in the following ways:

- The computing co-ordinator reports to governors when a full monitoring and evaluation is completed of Computing/E-safety.
- The Headteacher reports to governors termly on progress towards objectives within the school improvement plan.
- The governors are given the opportunity to approve the E-Safety Policy and review the effectiveness of the policy.

Designated Safeguarding Persons

Any designated safeguarding person should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data.
• access to illegal / inappropriate materials.
• inappropriate on-line contact with adults / strangers.
• potential or actual incidents of grooming.
• cyber-bullying.

Parents

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through the school website, parent evenings and newsletters. Year 5/6 parents may also invited to attend an annual e-safety workshop.

Parents/Guardians will be responsible for:

• supporting the school in promoting e-safety and endorsing the Parents' Acceptable Use Agreement (see Appendix 2) which includes the pupils' use of the Internet and the school's use of photographic and video images.
• reading, understanding and promoting the school Pupil Acceptable Use Agreement with their children.
• consulting with the school if they have concerns about their children's use of technology.

Pupils

It is important that all pupils at Churchtown Primary school:

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's / academy's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

• Policy to be posted on the school website with hard copies available from school on request.
• Policy to be part of school induction pack for new staff.
• Acceptable use agreements discussed with pupils at the start of each year.
• Acceptable use agreements to be recorded by the office and kept in teacher files.

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
• Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
• Any digital communication between staff and pupils (email on Purple Mash or Knowledge Box etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
• Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approaches To Teaching and Learning

E-safety is embedded into the curriculum and is covered through Computing and PSHE objectives.

Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Pupils will be expected to know school rules and understand school policies for bullying and behaviour, this is reinforced through circle time and Internet Safety Week.

Pupils should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Handling complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

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

• Interview with teacher/ Computing Subject Leaders/ SLT / Headteacher;
• Informing parents or carers;

• Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including online homework];
• Referral to LA / Police.

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

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

Review and Monitoring

The e-safety policy is referenced from within other school policies:

- The school has a computing subject leader who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the computing subject leader and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safety policy will be discussed in detail with all members of teaching staff.

Planning and Organisation

E-safety should be focused upon in all areas of the curriculum and staff should reinforce e-safety messages during computing lessons. The Computing Subject Leader has a clear, progressive and up-to-date e-safety education programme as part of the Computing curriculum/E-safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience (see Appendix 3).

In the Foundation Stage, pupils are taught to not give out any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At Churchtown Primary School we do expect children of this age to be supervised whilst using the internet. Reception pupils take part in the school “Internet Safety Week” using age appropriate CEOP resources.

In Key Stage One, pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and make sure that an adult knows what they are doing online. Teachers model appropriate online behaviour when communicating with others.

There are four key messages taught at Key Stage One:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.
- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

In Key Stage Two, themes taught in Key Stage One are built upon. In addition, pupils are made aware of online experiences which could cause potential danger, e.g. use of social networking, gaming sites and downloading or installing new applications. Links are made between inappropriate sharing of personal information and the dangers this can pose in the real world. Relevant resources from CEOP, Childnet and SWGfL are used during "Internet Safety Week" and other resources can be accessed throughout the year on the school website. In Key Stage Two, children also develop their research skills, especially through use of their iPads. They are taught about plagerism and the need to upload copyright laws.

Resources

E-safety resources are mainly online E-safety websites - links are available on the school website. Information about new resources/websites are communicated to staff via email.

Inclusion

At Churchtown we believe that all our children should be given the opportunity to achieve as well as they can in everything they do.

Use of Personal Equipment - Children

Use of Facebook / Social networking sites

Children are not permitted to use social networking sites on school premises. Both on computers or mobile devices.

Use of Mobile Phones

Mobile devices must be switched off and remain in bags during the school day. Parents and pupils to sign a disclaimer form if they wish to bring a mobile device into school (see Appendix 3).

Mobile phones brought into school are entirely at the persons own risk. Churchtown Primary School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.

Email

Children currently use the closed messaging systems of Purplemash. Other messaging or e-mail solutions may be used when appropriate for a particular year group.

Cyber-Bullying

Internet Safety Week is held annually with up to date e-safety guidance. The school website has links to cyber-bullying advice. Incidents of cyber-bullying are dealt with by leadership team and communicated to parents where necessary.

Acceptable Use Policy (AUP)
Staff members and Governors also have an AUP which is signed annually (Appendix 1).
All KS2 pupils during the Autumn term of the school year take home an AUP and then return it to schools signed by parents/guardians.
Both AUP's will be reviewed annually.

Incident Management
In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support will be actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing Subject Leaders, Infrastructure Manager or Leadership Team.
- all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Computing Subject Leader and Infrastructure Manager.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. This will be viewed where cause is justified (in line with the Behaviour Policy) and will only be viewed by the person leading the investigation.

Appendix 1:

Acceptable Use Policy
Staff, Governors and Visitors

ICT and the related technologies such as email, 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.

- I understand that personal devices should be kept in bags/cupboards and not out on desks. Mobile phone can be used in the staffroom and classrooms when the children are not present, but should not be used when walking around school or in places where children are.
- I understand that personal mobile phone calls/messages may only be taken during staff breaks or in staff members' own time. If staff need to have their phones for emergency use, they should notify the Leadership Team.
- I will not access facebook or other social networking sites from a school computer whilst on school premises. Facebook can be accessed on personal handheld devices at break times only.
- I will only use the school's email / Internet 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 and use appropriate language.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission of the network manager, Alistair West.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff must only be taken and stored on computers / drivers owned by the school.Images will not be distributed outside the school network (eg. Website / local press / Smugmug) 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 support the school approach to online safety and not deliberately upload or add any images, video,sounds or text that could upset or offend any member of the school community
- 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.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not access Facebook or other social networking sites from a school computer whilst on
- school premises. Facebook can be accessed on personal handheld devices at break times only.

Social Networking

Online conduct should not be different to offline conduct.

Employees using social networking sites in a personal capacity must ensure that they do not conduct themselves in a way that is detrimental to the School/College. To do otherwise may lead to formal disciplinary action under the School's/College's Disciplinary Procedure.
They should not:

- Post offensive, defamatory or inappropriate comments about the School/College, its students, suppliers or any of its employees.
- Allow interaction on websites to damage or compromise working relationships with colleagues
- Make discriminatory or offensive comments about work colleagues or students.

- Post photographs/videos of themselves, colleagues or students taken in school or which is work related unless agreed by the Headteacher.
- Post or send abusive or defamatory messages.
- Record any confidential information about the School/College on any social networking sites
- Post information which would lead to the identification of a student.
- Accept requests of any pupil of the School /College or former pupils under the age of eighteen to become ‘friends’ on Facebook or any other social networking site.
- It is advisable not to accept requests from the parents or guardians of any pupil of the School/ College or former pupils under the age of eighteen to become ‘friends’ on Facebook or any other social networking site. Should you wish to accept such a request you must seek advice from your Headteacher before doing so.
- Make a request to become ‘friends’ with any pupil of the School/College or former pupils under the age of eighteen as friends on Facebook or any other social networking site.
- Make a request to the parents or guardians of any pupil of the School/College or former pupils under the age of eighteen to become ‘friends’ on Facebook or any other social networking sites.
- It may be is necessary to create closed ‘blogs’ and social networking areas for curriculum purposes. Any such activity should be agreed in advance with the Headteacher.
- On occasions when it is appropriate for staff and students to share a closed ‘blog’ or social network area for curriculum purposes and permission has been given to do so, appropriate measures must be put in place to ensure the safety of the staff and pupils.
- Profiles on social media should not be traceable to a person’s place of work.

User Signature
I have read above statements and Sefton Councils Social Media Policy and I agree to follow this code of conduct and to support the safe and appropriate use of ICT throughout the school and in my online activity.

Signature ……..…….…… Date ……

Full Name …….....(printed)

Appendix 2:

Dear Parent/Guardian,

At Churchtown Primary School, ICT, including the Internet, email, i-pads and mobile technologies; play an important role across the curriculum. We expect all children to be safe and responsible when using any form of ICT.

Please read and discuss these e-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like further information please contact your class teacher .

Pupil Acceptable Use Policy

All pupils must follow the rules set out in this policy when using school computers, hand held devices and websites recommended by the school.

- I must not write anything that might upset someone or give the school a bad name.
- I know that the adults supervising me will regularly check what I have done on the school computers/i-pads.
- I must not tell anyone my name, where I live, or my telephone number when using the Internet.
- I must never use other people's usernames and passwords, or computers left logged in by them.
- If I think someone has been using my computer log in then I will tell my teacher.
- I must log off after I have finished with my computer.
- I must not use the computers in any way that stops other people using them.
- I will only access websites that have been recommended by my teacher.
- I will report any websites that make me feel uncomfortable to my teacher
- I will tell my parents or my teacher straight away if I am sent any messages that make me feel uncomfortable at home or at school.
- I will not try to harm any equipment or the work of another person on a computer.
- If I find something that I think I should not be able to see, I must tell the adult supervising me straight away and not show it to other pupils.
- If I have a mobile phone in school, I must complete the school's consent form and keep it turned off and in my bag during school hours.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

Using a computer with another person's username and password.

Creating or sending any messages that might upset other people.

Accessing websites that have not been checked by an appropriate adult first.

Please Return to Class Teacher

…….. (child's name) has discussed and agreed to follow the E-Safety rules, to support the safe use of ICT at Churchtown Primary School.

Parent/Guardian Signature ……

Child's Signature …… Class …… Date ……

Appendix 3:

Year 5 & 6 Mobile Phone Permission Form

The use of mobile phones in school is strongly discouraged. **The school cannot take responsibility for loss or damage to phones.**

It is recognised that some pupils do require mobile phones for their journeys to and from school. Under these circumstances mobile phones may be switched on and used outside normal school hours.

If a phone is activated during school hours, without the permission of a member of staff, it will be confiscated for the rest of that school day. If the mobile phone is used inappropriately, i.e. taking photographs or videos without permission, this privilege will be removed.

Parent/Guardian Permission

I have read and understand the above information about appropriate use of mobile phones at Churchtown Primary School. I understand that this form will be kept on file at the school and that the details may be used (and shared with a third party) to assist in the identification of a phone should the need arise (e.g. if lost, or if the phone is being used inappropriately).

I give my child permission to carry a mobile phone to school and understand that my child will be responsible for ensuring that the mobile phone is used appropriately and correctly.

I understand that the school accepts no responsibility for pupils who lose or have their mobile phones stolen.

Parent name (print) _____

Parent signature _____

Date _____

Pupil name (print) _____

Mobile phone number _____

Pupil signature _____

Date _____