

Werrington Primary
Werrington Primary
 School
School

e-Safety and Acceptable Use Policy

Editions & Revisions

May 2010	Bethany Windsor & Jamie Efford
November 2012	Ellie Henderson
Update January 2013	Ellie Henderson/BW Headteacher
Update November 2014	BW Headteacher
Update Sept2016	BW Headteacher
Reviewed Oct 17 Resources	Next review Oct 2018
Reviewed FGB Nov 18	Next review Nov 19

Werrington Primary School e-Safety and Acceptable Use Policy

This policy should be read in conjunction with:

Keeping Children Safe in Education (DFE September 2019),

The School Code of Conduct, Anti Bullying and Harassment and Equal Opportunities policies,

Computing 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. 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.

Computing Technology covers a wide range of resources including, web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Wikis and Tweepers
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Tablets and Chrome Books
- Other mobile devices with web functionality.

Whilst exciting and beneficial both in and out of the context of education, computing technologies particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At **Werrington Primary 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.

Both this policy and the Acceptable Use Agreement (for staff, governors, visitors and pupils – see appendices 1 and 2) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, Chrome Books, webcams, whiteboards, digital video equipment etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players etc.).

All users of the Werrington Primary School Network agree to the acceptable use policy when they log in.

Equal Opportunities

This policy should be read in conjunction with the school's equality Policy under the equality act 2010.

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues
- New staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children

within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)

- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year and an acceptable use statement is displayed when all users sign on to the school network.
- E-safety posters are prominently displayed.

e-Safety in the Curriculum

- The school has a framework for teaching internet and communications skills in Computing.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety guidance linked to the curriculum .
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- Teachers are directed to actively re-visit the acceptable use statement which appears when a child logs into the school server.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Peterborough City Council and E2BN monitor searches and sites visited and SECURUS is used at Werrington Primary School to ensure staff and pupil use of computer technology is monitored.. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- SECURUS flagged incidents will be followed up appropriately.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, Google Chrome Books, iPads, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to

manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

Any visitors to the school including parents will be asked to turn off their mobile phone whilst on the school premises and asked to refrain from using them.

Whilst the school allows staff to bring in personal mobile phones and devices for their own use there are acceptable times when their use is allowed eg. during breaktime, lunchtime and when pupils have left the school. Areas in school where they can be carried and used which offer privacy are: general office areas the staff room, classrooms BUT ONLY when pupils are not present at the end of the school day. Mobile phones must not be used when supervising or working with pupils including in before/after school clubs. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. Staff Mobile phones should be turned off and stored securely in a personal bag, locker or cupboard preventing inadvertent use. Staff should not walk around school with a mobile phone about their person.

- The school does not allow pupils to bring personal mobile phones to school and is not responsible for the loss, damage or theft of any brought in. Parents/Carers should discuss any concerns regarding this with school.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones) for visits and residential trips

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used. This will include the use of 3G enabled devices to update the school Twitter account for example on day trips and residential visits. Any photographs taken on the appropriate school device must be deleted once it has been published or use in accordance with school expectation and guidance. The school has provided a mobile phone which is capable of taking photographs and iPad technology for taking photographs, updating the school website and Twitter communication.

In the event of an emergency Staff may use a personal mobile phone to contact emergency services, the school or other appropriate agency. The school mobile should be used in the first instance however it is recognized that the use of additional staff phones in such emergencies could be useful and appropriate.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good netiquette.

- The school gives all staff their own email account to use for all school business using Office 365 - anywhere/device This is to minimise the risk of receiving unsolicited or malicious emails 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 email histories can be traced. This

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 email addresses.
- E-mail sent to an external organisation should be written 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.
- Children use a class/ group email address or their gmail address with express permission from a member of staff . The gmail address may only be used for agreed school purposes.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) 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 or use inappropriate language or derogatory terms.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform their Team Leader or Headteacher if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

Safe Use of Images Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others. .

School Performances and events

Parents/Carers and family visitors attending school assemblies and performances will be managed whilst on school site to and from the performance area thus preventing inadvertent use of photograph enabled technologies. All Parents/Carers/Family Related visitors sign the Performance Photography book which states that photographs taken during school performances or events must only be used for private use and must not be shared more widely including within social media.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas including external events, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- for training purposes

- for transition purposes and shared with next providers eg secondary school

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/Carers may withdraw permission, in writing, at any time. Update forms are forwarded to parents each year giving the opportunity to revise consents. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ server or other storage.

Google Chrome Books and pupil Google accounts

- Pupils are expected to use their school Google account responsibly and where this is found not to be the case, measures will be put in place to monitor this more fully or remove access.
- Chrome books are expected to be a tool for accessing pupil work via Google accounts and pupils are expected to use this technology responsibly including when collaborating with other pupil's work.

Webcams

- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the, inappropriate materials section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing – not currently undertaken

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Social Networking

Social Networking has become part of our society with the rise of Facebook and Twitter, however we

must ensure that children remain safe whilst online. Many of these social networking sites are blocked through our secure internet system with the exception of twitter. Twitter is only used with the supervision of adults and with school/class based logons.

The school recognises that many staff will actively use Facebook, Twitter and other such social networking sites, blogging and messaging services. Staff must not post material (including text, video, audio or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Those who post material, which could be considered as inappropriate, could render themselves vulnerable to criticism or allegations of misconduct.

It is never permissible to accept a friendship request from pupils at the school, as in almost all cases, children of primary age using such networks will be breaching terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still in education. If a parent seeks to establish contact, the member of staff should exercise their professional judgment. Under no circumstances should pupils be accepted as on-line friends of members of staff.

Any policy breach will be subject to the school's disciplinary policy and code of conduct.

All staff, governors and volunteers will read Part 1 of Keeping Children Safe in Education (2019) and any other recommended documents including The School Code of Conduct to ensure they are familiar with the signs and symptoms of abuse.

Misuse and Infringements Complaints

Complaints relating to e-Safety should be made to the Headteacher. Incidents should be logged. Facebook, BBM, IM, email and text can be used to insult, verbally attack and harass causing unacceptable stress and upset for members of staff as well as pupils in such circumstances. All incidents must be reported to enable full investigation as well as support to the victim of such behaviour.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher. This is also reinforced with SECURUS monitoring software.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged on the seriousness of the offence; investigation by the Headteacher/ LA and Governors will be instigated and the involvement of the Police may be considered when a breach of this policy is deemed.
- Users are made aware of sanctions relating to the misuse or misconduct by the Headteacher.

Equal Opportunities Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents / carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy in writing.
- Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
 - o Information and celebration evenings
 - o Posters
 - o Website/ Learning Platform postings
 - o Newsletter items

Writing and Reviewing this Policy Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making / reviewing the e-Safety policy through school council meetings, assemblies and staff meetings

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. The policy will be amended if new technologies are adopted and in response to Keeping Children Safe in Education – KCSIE September 2019.

Computing Lead Teacher: Mr Pope

Headteacher/Co-Headteacher : Mr Wilding/Mrs Simmons

Chair of Governors: Chris Pennell

**Werrington Primary School
Primary Pupil Acceptable Use
Agreement / e-Safety Rules**

Dear Parent/ Carer,

Computing including the internet, email and mobile technologies have become an important part of learning in our school. We expect all children to be safe and responsible when using any computing technologies. 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 some explanation please contact the Computing Lead Teacher or the Headteacher.

- I will only use Computing Technology in school for school purposes.
- I will only use my school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my Computing passwords.
- I will only open or delete my own files.
- I will make sure that all Computing 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 Computing because I know that these rules are to keep me safe.
- I know that my use of Computing can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.
- I will use my Google account responsibly and follow the same guidelines that apply in school.

Parent/Carer signature

We have discussed this and (child’s name) agrees to follow the e-Safety rules and to support the safe use of Computing at Werrington Primary School.

Parent/ Carer Signature

Class.....

Date.....

**Werrington Primary School
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct**

All staff, governors and volunteers will read Part 1 of Keeping Children Safe in Education (2019) and any other recommended documents to ensure they are familiar with the signs and symptoms of abuse. A record will be kept to demonstrate compliance.

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of Computing in connection with school business. All staff and Governors are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the lead Computing Lead Teacher – Mr Pope 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 Headteacher or Governing Body (including any email communications between a Governor and the school office/staff).
- I will comply with the Computing 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 or in line with The Code of Conduct Policy for all Adults and report any incidents where I believe a third party’s conduct has breached this agreement.
- 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 Integris G2/Target Tracker) 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 Headteacher or Governing Body

I will ensure that I comply with ‘General Data Protection Regulation 2018 in safeguarding personal data’ I will not install any hardware or software without permission of the Headteacher

- 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 agreement 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 schools e-Safety agreement and help pupils to be safe and responsible in their use of Computing and related technologies. I will ensure the guidance found in KCSIE September 2019 is followed.

User Signature

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

Signature

Date

Full Name(printed)

Job title