Winterton Junior School E-Safety Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. At Winterton Junior School we believe that all children should be taught to use the internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.
Ofsted (ref 2013) identified the main risks to our school community, these can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games, substance abuse, racism, hacking and information dump web sites.
- 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.
- Online bullying.
- Identity theft.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being from the perspective of the amount of time spent online including gaming.
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Extremism.
- Copyright.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other school policies (e.g. behaviour, safeguarding, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, governors, community users) who have access to and are users of school IT systems, both in and out of 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 out of school, but is linked to membership of the school. 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.

The purpose of this document is to address the concerns set out by Ofsted and Winterton Junior School that:

- Set out the key principles expected of all members of the school community at Winterton Junior School with respect to the use of IT-based technologies.
  Safeguard and protect the children and staff of Winterton Junior 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 educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying, which are cross-referenced with other school policies.
- Ensure that 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.

Roles and Responsibilities

1. **Head teacher and Senior Leaders:**

- The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day-to-day responsibility for E-Safety will be delegated to the E-Safety Officer.
- The Head teacher/Senior Leaders are responsible for ensuring that the E-Safety Officer 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 Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role.
- The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the E-Safety Officer.
- The Head teacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety incident or allegation being made against a member of staff.
- To take overall responsibility for data and data security.
- To take overall responsibility for the business continuity plan.
- To ensure the school uses an approved filtered Internet Service, which complies with current statutory requirements.
- Liaises with the Local Authority and relevant agencies.

2. **E-Safety Officer**

- Leads on e-Safety.
- Takes day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Facilitates training and advice for staff.
- Liaises with school IT technical staff.
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Reports regularly to Senior Leadership Team.
- Liaises with the Local Authority and relevant agencies.
- Promotes an awareness and commitment to Online safeguarding throughout the school community.
- Ensures that Online safety education is embedded across the curriculum.
- To ensure that an Online safety incident log is kept up to date.

3. Technical support staff / School Network Manager

These staff are responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the school's networks through a properly enforced password protection policy.
- Promotes an awareness and commitment to Online safeguarding throughout the school community.
- Liaises with the Local Authority and relevant agencies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- To ensure that an Online safety incident log is kept up to date.
- Facilitates training and advice for staff.
- The school's filtering policy is applied and updated on a regular basis.
- That he/she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- That monitoring software/systems are implemented and updated as agreed in school policies.
- Is regularly updated in E-Safety issues and legislation, and be aware of the potential for serious child protection 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.
- Online bullying and use of social media.
- To report any online safety related issues that arise coordinator.
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.
- To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date).
- To maintain the security of the school IT system.
- To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices.
- The school's policy on web filtering is applied and updated on a regular basis.
- Inform and update others as relevant regarding technical and safeguarding changes.
- Reports regularly to Senior Leadership Team.
- Monitors the school infrastructure regularly in order that any misuse/attempted misuse can be reported to the Headteacher.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's online security and technical procedures.

4. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- They have read and understood and signed the school Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem (completing log template) to the appropriate person for investigation.
- Digital communications with students/pupils (e-mail/Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school communication systems.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Students/pupils understand and follow the school E-Safety and acceptable use policy.
- Students/pupils have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school 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.
- To model safe, responsible and professional behaviours in their own use of technology.

5. Designated senior person(s) for child protection

Staff should be trained in e-Safety issues and be aware of the potential for serious child protection 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.
- Potential or actual incidents of extremism/radicalisation.
- Cyber-bullying.

6. Students/pupils

- Are responsible for using the school IT systems in accordance with the Student/Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 carry this out.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To help the school in the creation/ review of e-safety policies/pupil Acceptable Usage Agreement.

7. Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate and safe way. The school will therefore take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, website and information about national/local E-Safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy.
- Accessing the school website in accordance with the relevant school Acceptable Use Policy.
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children.
- To consult with the school if they have any concerns about their children's use of technology.

8. Computing Curriculum Leader

- To oversee the delivery of the online safety element of the Computing curriculum.
- To liaise with the IT coordinator regularly.

9. Governors/Online Safety Governor

- To ensure that the school follows all current Online safety advice to keep the children and staff safe.
- To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Sub Committee receiving regular information about online safety incidents

and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities.
- The role of the Online Safety Governor will include:
- Regular review with the Online Safety Co-ordinator/Officer (including Online safety incident logs, filtering/change control logs).

10. Data Manager
- To ensure that all data held on pupils on the school office machines have appropriate access controls in place.

11. External groups
- Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication

The policy will be communicated to staff/student/community in the following ways:
- Policy to be posted on the school website/wintranet/staffroom/classrooms.
- 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 issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Education and Curriculum
- A planned E-Safety programme will be provided as part of Computing/PSHE/other lessons and should be revisited regularly – this will cover both the use of IT and new technologies in and beyond school.
- Key E-Safety messages should be reinforced and revisited as part of a planned programme of assemblies and pastoral activities.
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of any information.
- Students/pupils should be helped to understand the need for the student/pupil AUP and encouraged to adopt safe and responsible use of IT, the Internet and mobile devices at all times both within and outside school.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright.
- Rules for use of IT systems / Internet will be posted in all classrooms:
- *We ask permission before using the Internet.*
- *We try to check the reliability of information.*
- *We only use websites or apps our teachers have chosen for us.*
- *We tell an adult if we see anything we are uncomfortable with- do not delete.*
- *We will not look at, move or delete other people's files without their permission.*
- *We only e-mail or message people our teachers have approved.*
- *We only send emails and messages that are polite and friendly.*
- *We never give out any personal information (including photographs) or passwords – including 'pop ups.'*
- *We never arrange to meet anyone we don't know.*
- *We do not open files or emails sent by anyone we don't know.*
- *We do not use Internet chat rooms.*
- *I will not respond to or add people I do not know personally.*
- *I will not use mobile phones in school; I will leave mine in the office if I bring it to school.*
- Staff should act as good role models in their use of IT, the Internet and mobile devices.

Education & Training – Staff

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal E-Safety training will be made available to staff where possible/required. An audit of the e-Safety training needs of all staff will be carried out regularly. It is possible/likely that some staff will identify E-Safety as a training need within the performance management process.
- All new staff/trainees should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Policies.
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

Training – School Governors

- School Governors have an awareness of e-Safety and how this is applied and implemented in school.
- School Governors to be invited to take part in relevant e-Safety training/awareness sessions.
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

Managing the IT and Computing infrastructure

This school:

- Uses the TINA filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the students.
- Ensures network healthy through use of Sophos anti-virus software etc. and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA or Winterton Junior School approved systems to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable/useful.
- Works in partnership with other parties to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search, …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored;.
- Informs staff and students that that they must report any failure of the filtering systems directly to the e-Safety officer/IT technician.
- Our e-Safety officer/IT technician logs or escalates as appropriate to the LA Helpdesk as necessary.

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school:

- Uses audited year group log-ins for students and individual log-ins for staff.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Ensures the IT technician is up to with changes in technology and policies that affect or embellish the curriculum.
- Storage of all data within the school will conform to the UK data protection requirements.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU. All technologies that do not store their data in the EU must not be used unless the express permission from the head teacher is given.

To ensure the network is used safely

This school:

- Ensures staff read and sign that they have understood the school's e-Safety Policy. Following this, they are set-up with Internet, and network access.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- We provide pupils with a year group log on name.
- Makes clear that staff should not log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files/programmes.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager/TA; equipment installed and checked by approved Suppliers/LA electrical engineers.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems.

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements.
- Uses the DfE secure S2S website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school IT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong password.
- We require staff to change their passwords at least three times a year.
- The "master/administrator" passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leaders.

Digital images and videos

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs/
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file) that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;.
- Uploading of information is restricted to our website authorisers.
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website unless specific permission has been gained.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

The Use of E-mail.

There are responsibilities involved in using e-mail. In signing the Agency Acceptable Use Policy all employees agree to fulfil these responsibilities. All staff are allocated a "@wintertonjuniorschool" e-mail address when they join the school. This e-mail address should be used for all official e-mails.

General Considerations when using E-mail

E-mail is not a confidential means of communication. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and in particular recognise that e-mails can be:

- Intercepted by third parties (legally or otherwise).
- Wrongly addressed.
- Forwarded accidentally.
- Forwarded by initial recipients to third parties against your wishes.
- Viewed accidentally on recipients' computer screens.
- Sensitive personal data should not be communicated by e-mail unless permission of the subject has been obtained or unless encryption facilities have been employed. We use secure, LA/DfE approved systems S2S.
- Staff must not include any defamatory comments in any e-mail messages. Email is a form of publication and the laws relating to defamation apply.
- Staff must never use a false identity in e-mails, and must be aware that there is no guarantee that e-mail received was in fact sent by the stated sender. If, for any reason, an e-mail is sent on behalf of someone else the sender must make that clear at the beginning of the message.
- The e-mail system must not be used to create or distribute offensive or unwanted e-mail.
- E-mail messages that show Winterton Junior School in an unprofessional light or that could expose it to legal liability must not be sent by any member of staff.
- Be very careful when downloading material from the Internet and opening external e-mails if there is any suspicion of it including a virus. If you have any suspicions, do not open an attachment and contact IT Technical Support Officer immediately.
- Staff must not invade anyone's privacy using e-mail.
- E-mail is not a substitute for record-keeping purposes. Where accessibility is an issue staff must transfer e-mail records to a more lasting encrypted medium.
- The laws applying to copyright apply to e-mail messages and attachments. Staff must familiarise themselves with policies in relation to copyright.

Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style'.

- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- The sending of chain letters is not permitted.

- Embedding adverts is not allowed.
- All staff sign our Acceptable Usage Agreement (AUP) to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Pupils

Pupils are introduced to, and use e-mail as part of the IT/Computing scheme of work. Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

- Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- That an e-mail is a form of publishing where the message should be clear, short and concise.
- That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- That they should think carefully before sending any attachments.
- Embedding adverts is not allowed.
- That they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
- Not to respond to malicious or threatening messages.
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- That forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Social Networking

Acceptable use of social networking sites

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The requirements set out below aim to support innovation whilst providing a framework of good practice.

Social networking applications include, but are not limited to:

- Blogs.
- Online discussion forums.
- Collaborative spaces.
- Media sharing services e.g. Youtube.
- 'Micro logging' applications e.g. Twitter.

Use in Schools

The use of social networking sites within school is only allowed in appropriately controlled situations and in support of curriculum activities – for example to teach the safe use of the Internet.

- Staff and students must not access social networking sites for personal use via school information systems, school networks or using school equipment.
- If staff access social networking sites it must be using their personal computer systems and equipment.
- Staff must not place inappropriate photographs on any social network space. Photographs of colleagues and/or pupils - taken for example on school trips - must not be posted without the express permission of those in the photographs or their parents/carers.
- Staff are strongly advised not to communicate with students over social network sites using their personal systems and equipment.
- Staff must not run social network spaces for student use on a personal basis.

- Schools are vulnerable to material posted about them online and all staff will be made aware of the need to report this should they learn of anything bringing the school into disrepute. Schools are advised to check regularly, using a search engine, to see if any such material has been posted.

If staff use social networking sites they should not publish specific "personal views" relating to the school, staff or students.

The school network and IT facilities must not be used for the following activities:
- Conducting illegal activities.
- Accessing or downloading pornographic material.
- Gambling.
- Soliciting for personal gain or profit.
- Managing or providing a business or service.
- Revealing or publicising confidential information.
- Representing personal opinions as those of the school.
- Making or posting indecent or offensive remarks or proposals.

School staff will ensure that in private use:
- No reference should be made in social media to students/pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Enforcement
Winterton Junior School reserves the right to require the closure or removal of content published by representatives which may negatively affect the reputation of the school or put it at risk of legal action. Any communications or content you publish that causes damage to Winterton Junior School or any of its employees reputation may amount to Disciplinary Policies applying.

Data Protection
The Data Protection Act (DPA) applies to all establishments wherever located.

Staff must ensure that they:
- Keep personal data in a secure environment, reducing the risk of loss or misuse.
- Use personal data only on secure, password-protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session.
- Transfer data using encryption and secure password protected devices.

When using communication technologies schools must consider the following as good practice:
- Users need to be aware that emails are not secure and can be monitored.
- Users must immediately report, to the nominated person, any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not reply to any such e-mail.
- Any digital communication between staff and students/pupils or parents/carers must be professional in tone and content.

Data security: Management Information System access and Data transfer
Strategic and operational practices
At this school:
- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners <in a spreadsheet>.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

- Staff.
- Governors.
- Pupils.
- Parents.

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer.
- We use ‹encrypted flash drives› if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are managed by DBS checked staff.
- We backup servers to Winterton Junior school backup solution.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and ‹get a certificate of secure deletion for any server that once contained personal data.
- Paper based sensitive information is shredded, using cross cut shredder/collected by secure data disposal service.
- We are using secure file deletion software. Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

Equipment and Digital Content

Personal mobile phones and mobile devices:

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored at the office (reception) on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- 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. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the Headteacher.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally owned device into school. Any device brought into school must be handed in to the office at the start of the day.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make and model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Misuse

Misuse of school electronic equipment is a serious disciplinary offence.

The Headteacher can exercise a right to monitor the use of a school's information systems and Internet access. This includes the right to intercept email and delete inappropriate materials where unauthorised use of the school's information system may be taking place. Staff must be aware that improper or unacceptable use of the Internet, email and equipment could result in legal proceedings and the use of the school's Disciplinary Procedure. Sanctions will depend upon the misuse and could result in dismissal. If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately. Allegations against Staff Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Misuse by pupils

Should a pupil be found to misuse on-line facilities whilst at school the following consequences will occur:

- Any child found to be purposely misusing the Internet by not following the Acceptable Use Agreement will have a letter sent home to parents/carers explaining the reason for suspending the child's use for a particular lesson or activity.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally views inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen, so that an adult can take the appropriate action (log to be made where necessary). Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. Children should be taught and encouraged to consider the implications for misusing the Internet.

Incidents

Any E-safety incident is to be brought to the attention of the E-Safety Officer, or the Headteacher. The E-Safety Officer will assist you in dealing with the incident and to fill out an incident log.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

- Report to and discuss with the named child protection officer in school, Local Authority Designated Officer (LADO) (where appropriate) and contact parents/carers.
- Advise the child on how to terminate the communication and save all evidence.
- Contact CEOP http://www.ceop.gov.uk/
- Consider the involvement of police and social services.
- Inform LA e-safety officer.

Responding to 'serious' incidents of misuse:

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

- Have more than one senior member of staff/volunteer involved. This is to protect individuals if accusations are reported.
- Conduct the procedure using a designated computer that will not be used by pupils and if necessary can be taken off site by the police. 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 carry out the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form/log (except in the case of images of child sexual abuse - see below).

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be stopped and referred to the Police immediately. Other instances to report to the Police would include:

- Incidents of 'grooming' and terror/radicalisation related behaviour.
- The sending of obscene materials to a child.
- Adult material that potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

In such cases, isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken, they will provide an evidence trail for the school and possibly the police and demonstrate that visits/viewings to these sites were carried out for child protection purposes. Ensure a detailed log is completed.

Expected conduct

In this school, all users:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Agreement/Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on online bullying.

Staff

- Are responsible for reading the school's E-Safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

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.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in E-Safety within the school. The records are reviewed/audited and reported to the school's senior leaders/Governors/the LA/LSCB.
- Parents/carers are specifically informed of online 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.

Asset disposal

- Details of all school owned hardware will be recorded in a hardware inventory.
- Details of all school owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

WINTERTON JUNIOR SCHOOL

Acceptable Use Policy

Winterton Junior School recognises the importance of the correct usage of technology within the curriculum. To help ensure that technology is used in a safe and appropriate manner, it is important to have an acceptable use policy for all users that details what is acceptable and unacceptable usage. The acceptable use policy covers any ICT device/system located within Winterton Junior School, including the wireless infrastructure and all forms of paper and digital technologies, for example but not limited to, Internet, Intranet, network resources, software and school data.

Aims of this policy

This acceptable use policy is intended to ensure within Winterton Junior School:

- That staff, governors and volunteers will be responsible safe users.
- That staff, governors and volunteers are proactive in minimising any potential risk whilst using ICT devices/systems.

Winterton Junior School will always strive to ensure that users have suitable access to ICT devices to enhance their work, to enhance learning opportunities and will, in return expect staff, governors and volunteers to be a responsible safe user.

Acceptable use policy agreement

I understand that to use any ICT device/System located within Winterton Junior School I must have read, accepted and signed the acceptable use policy. This will help ensure that risk to myself, ICT devices/system and of other users minimised, and that that I stay safe and that I promote safety and security of the ICT devices/systems and of other users.

Professional and personal safety

- I understand that Winterton Junior School log all activity when I use any school ICT device/system and that the Headteacher can gain access to this information if necessary as well external agencies such as the police using a RIPA (regulation of investigatory powers act) request.
- I understand that Winterton Junior School IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will notify the head and IT staff immediately. I will ensure I change it as required every 90 days. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access any school or LA ICT system/device. I will ensure all documents and data are printed, saved, accessed and deleted/shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities or ethics.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission; this includes content on the internet.

- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree that I must read the business continuity plan.
- I understand my responsibilities fully in the business continuity plan.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- Teaching staff only - I will embed the school's E-Safety/digital literacy/counter extremism curriculum into my teaching.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Head teacher or SLT member.
- I will alert the child protection officer/appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I will not store any school information on any cloud providers network unless express permission is given by the Headteacher.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher.

Using and accessing Winterton Junior school ICT devices/systems

- I will not download any software or resources from the Internet that can compromise the network or that might allow me to bypass the filtering and security system or are not adequately licensed.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's Sophos antivirus.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home without permission from the Headteacher.
- I will not create any personal wireless "hot spots" on Winterton Junior School grounds.
- I will follow the school's policy on use of mobile phones/devices at school.
- I will try not to download or upload large files that might "swamp" the Internet connection and prevent other from accessing in the Internet.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff drive located on the school network.
- I agree and accept that any computer or laptop loaned to me by the school, is provided to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any local authority system(s) I have access to in accordance with their policies.
- I understand that any work created by myself belongs to Winterton Junior School from a copyright perspective. I agree to notify the head teacher if I want to use any school content/data outside of school use.
- I agree to only use USB memory sticks (encrypted or non-encrypted) to transport data to and from site. Once a USB memory stick inserted into a computer I will copy/move this data onto the staff shared area or my private network home drive.
- I understand that my teaching and learning resources must be located on the staff shared area or my private network home drive so that the school can retrieve this work should an issue or a business continuity event occur.
- I understand that my private network home drive is viewable by the network backup software and where appropriate the school IT technicians.

- I understand that permission will be sort from the head teacher should access to my private network home drive become necessary.
- I understand that any private data encryption keys generated by myself to be used for Winterton Junior School will be given to the school IT technicians. If I do not and the data is lost I understand that I accept full responsibility including any monetary costs to retrieve that data.
- I understand that I will give my encrypted USB memory stick pin code to the Business Manager and that the pin code will be stored securely in the fire safe.
- I understand the importance to report any all faults using the support desk function on the http://Wintranet.
- I understand to notify the school IT technicians or SLT member(s) (if the school IT technicians are unavailable) immediately should a warning appear regarding malware, spyware, Trojans or any other computer viruses.
- I understand I will disconnect any equipment immediately should a virus warning appear on any computer or device whilst I am using it. If you are unsure about how to disconnect a device from the network, log off (if appropriate), switch the equipment off and immediately notify the school IT technicians or SLT member(s) (if the school IT technicians are unavailable).
- I will not discuss the technical setup of the devices/systems outside of school in great detail unless express permission from the head is given.
- I will ensure that the wireless access key is not given out to students, visitors or 3rd parties unless express permission from the head is given.
- I will not disable or cause damage to any device/system.
- I will not install any software onto any device/system.
- I will not attempt to alter any software settings unless allowed for in the school policies.
- If I create content for the school on a computer(s) that does not belong to the school, I must ensure that the device/system is virus/malware free and that there is up to date antivirus running
- I will ensure my data is regularly (regularly is daily) backed up with the schools backup solution and software.
- I will not open any hyperlinks contained or attachments located in emails unless they appear genuine. Sometimes apparently genuine email can still contain viruses, spyware, malware and Trojans.
- I understand my responsibilities within the data protection act and that in essence it requires that any access or storing or digital information will be kept private and confidential unless required by the law and other agenises using such as powers as the RIPA act. Any data stored must only be kept for as long as the data is required.
- I will bring back any ICT device/system given to me before leaving the school unless express permission is given by the head teacher.
- I will use the provided office 365 staff email facility only unless permission is granted from the Headteacher.
- I will ensure I regularly clear out email folders that are is required by the data retention clause in the data protection act.
- I will not send any data to any third party without express permission by the Headteacher.
- I will not click on email links that I do not recognise and will immediately delete the email.
- I will not download attachments that I do not recognise.
- I will not download attachments onto a computer that is not running anti-virus software.
- I will not post school email addresses onto forums unless is necessary as part of your job function.

WINTERTON JUNIOR SCHOOL ACCEPTABLE USE AGREEMENT
for staff, volunteers and governors 2016

I sign to accept that I have read and fully understand the acceptable use policy. I understand if I do not follow the acceptable use policy that I may put myself in an unsafe position that could damage my position/reputation and that of the school.

Please print this final page twice and sign both copies. Keep copy 1 for yourself and give copy 2 to the Headteacher. Enter 1/2 into the field below.

Copy ☐

Name: _____

Role: _____

Signed: _____

Date:_____

WINTERTON JUNIOR SCHOOL ACCEPTABLE USE AGREEMENT
(Pupils) 2016

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the IT equipment, if I accidentally damage something I will tell my teacher.

I will not – share passwords with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever worried in school or my parents/carers if I am at home.

I understand – if I break the above rules there will be consequences of my actions and my parents/carers will be told.

Signed (Parent/Carer):_____

Signed (Student):_____

Date:_____

Winterton Junior School E-Safety Incident Log

Device Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		
Signature (Headteacher)		**Date:**
Signature (Governor)		**Date:**

Review and Monitoring

The E-Safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-Safety coordinator 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.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school policy will be discussed in detail with all members of teaching staff.

E-Safety Policy written by Gemaine Cooney/Clive Moore: September 2016
E-Safety Policy approved by Staff: Autumn 2016
E-Safety Policy Date approved by Governors: Autumn 2016
E-Safety Policy to be reviewed: Autumn 2019