Ormesby Primary School

Computing and Online Safety Policy

Issue Date:	May 2021
Reviewed:	April 2023
Author:	Mrs Michelle Loughran

IRONSTONE ACADEMY TRUST

Computing and Online Safety Policy

Introduction

At Ormesby Primary, we have an ever-evolving Computing curriculum, which aims to give children the transferable skills they need to be successful in an increasingly technology- focused world.

Through direct teaching, and through experience gained in other curriculum areas, children develop their skills in the following areas:

1. **Digital Citizenship** - the ability to communicate in a safe and respectful manner is our main priority in the teaching of computing skills.

2. **Digital Creator** - we teach children to be creative in the way they use technology to communicate their knowledge and understanding of the world.

   We teach children how to use technology to expand their knowledge, while at the same time teaching them how to do so safely and knowing how to find reliable information sources.

3. **Digital Communicator** - we teach children how to use technology to solve problems. Using a range of devices and software, we teach children the skills of problem solving, creativity and logical thinking which underpin the skills needed to program.

Aims

The school's aims are to:

- Provide a relevant, challenging and enjoyable computing curriculum for all pupils.
- Meet the requirements of the National Curriculum programmes of study for computing.
- Use computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.
- To equip pupils with the confidence and capability to use their computing skills and knowledge throughout their later life.
- To enhance learning in other areas of the curriculum using their understanding of computing.
- Provide efficiently for remote learning.
- To develop the understanding of how to be safe and responsible users of technology.

The National Curriculum for computing aims to ensure that all pupils:

- Can understand and apply the fundamental principles of computer science,including logic, algorithms, data representation, and communication
- Can analyse problems in computational terms, and have repeated practicalexperience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliartechnologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Rationale

The school believes that computing:

- Gives pupils immediate access to a rich source of materials.
- Can present information in new ways which help pupils understand access and use it more readily.
- Can motivate and enthuse pupils.
- Develop problem solving, logical reasoning and computational understanding.
- Mould children into adept digital citizens, digital creators and digital communicators.

Objectives

Early Years

It is important in the EYFS to give children a broad, play-based experience of Technology in a range of contexts, including outdoor play. Technology is not just about computers. Early yearslearning environments should feature Technology scenarios based on experience in the real world, such as in role play. Children gain confidence, physical skills and language skills through opportunities to 'paint' on the whiteboard, take & print photos using iPads or drive a remote-controlled toy. Outdoor exploration is an important aspect, supported by Technology toys such as metal detectors and walkie-talkie sets. Recording devices can support children to develop their communication skills.

ELG for the End of the Reception Year:

- Children recognise that a range of technology is used in places such as homes andschools. They select and use technology for particular purposes.

Key Stage One

By the end of Key Stage One pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digitaldevices, and that programs execute by following precise and unambiguous instructions.
- Create and debug simple programs.
- Use logical reasoning to predict the behaviour of simple programs.
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content.
- Recognise common uses of information technology beyond school.
- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content orcontact on the internet or other onlinetechnologies

Key Stage Two

By the end of Key Stage Two pupils should be taught to:

- Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output.
- Use logical reasoning to explain how some simple algorithms work and to detectand correct errors in algorithms and programs.
- Understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer forcommunication and collaboration.
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- Select, use and combine a variety of software (including internet services) on a rangeof digital devices to design and create a range of programs, systems and content thataccomplish given goals, including collecting, analysing, evaluating and presenting data and information.
- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Resources and Access

Planning

As the school develops its resources and expertise to deliver the computing curriculum, activities are planned in line with the National Curriculum and will allow for clear progression. Projects will be designed to enable pupils to achieve the stated objectives set out in the National Curriculum PoS for each key stage and the ELG. Pupil progress towards these objectives will be recorded by teachers as part of their class recording system.

Cross Curricular Links

As a staff, we are all aware that computing capability should be achieved through core and foundation subjects. Where appropriate, computing should be incorporated into schemes of work for all subjects. Computing should be used to support learning in other subjects as well as develop computing.

Assessment and Record Keeping (also see assessment policy)

Teachers regularly assess capability through observations and looking at completed work. Key objectives in the programming strand are taken from the National Curriculum to assess key computing skills each year and to track progress. Assessing computing work is an integral part of teaching and learning and central to good practice.

Monitoring and Evaluation

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching in line with the schools monitoring cycle. This may be through lesson observations, learning walks and feedback given from staff at standards meetings. The subject leader is also responsible for supporting colleagues in the teaching of computing, for being informed about current developments in the subject, and for providing a strategic leadand direction for the subject in the school. We allocate special time for the vital task of reviewing samples of children's work and for visiting classes to observe teaching in the subject.

Remote Learning

The schools remote learning offer is shared on the website and sets an expectation that we will provide a safe learning environment in which we will deliver a broad and balanced curriculum (See the Remote Learning Policy for more information).

Pupils with Special Educational Needs (see also SEND policy)

We believe that all children have the right to access computing. In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adaptthe delivery of the Computing Curriculum. We teach computing to all children, whatever their ability. Computing forms part of the National Curriculum to provide a broad and balanced education for all children. Through the teaching of computing, we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate computing can be used to support SEND children on a one-to-one basis where children receive additional support.

Equal Opportunities (see also equal opportunities policy)

At Ormesby Primary School will ensure that all children are provided with the same learning opportunities regardless of social class, gender, culture, race, disability or learning difficulties. As a result, we hope to enable all children to develop positive attitudes towards others. All pupils have equal access to computing and all staff members follow the equal opportunities policy. Resources for SEND children will be made available to support and challenge appropriately.

Roles and Responsibilities Computing Subject Leader

- There is a computing leader who is responsible for producing a computing development plan and for the implementation of the computing policy across the school.
- To offer help and support to all members of staff (including teaching assistants) in their teaching, planning and assessment of computing.
- To maintain resources and advise staff on the use of resources.
- To monitor classroom teaching or planning following the schools rolling programme of monitoring.
- To monitor the children's computing work, looking at samples of different abilities.
- To manage the computing budget.
- To lead staff training on new initiatives and update staff on changes.
- To attend appropriate in-service training and keep staff up to date with relevant in- formation and developments.
- To have enthusiasm for computing and encourage staff to share this enthusiasm.
- To keep parents and governors informed on the implementation of computing in the school.
- To liaise with all members of staff on how to reach and improve on agreed targets
- To help staff to use assessment to inform future planning.

The Role of the Class Teacher

Individual teachers will be responsible for ensuring that pupils in their classes have opportunities for learning computing skills and using computing across the curriculum. The class teacher will also complete the computing assessments to tracker to identify any 'gaps', which need addressing.

CPD

Staff Training

The computing subject leader will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year. Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the subject leader.

Health and Safety (see also health and safety policy)

The school is aware of the health and safety issues involved in children's use of resources. All fixed electrical appliances in school are tested by an external contractor every five years and all portable electrical equipment in school is tested by an external contractor every twelve months. It is advised that staff should not bring their own electrical equipment in to school, but if this is necessary, then the equipment must be pat tested before being used in school. This also appliesto any equipment brought in to school by, for example, people running workshops, activities, etc. and it is the responsibility of the member of staff organising the workshop, etc. to advise those people. All staff should visually check electrical equipment before they use it and take any damaged equipment out of use. Damaged equipment should then be reported to the senior sitetechnician, bursar or head teacher who will arrange for repair or disposal.

- Children should not put plugs into sockets or switch the sockets on.
- Trailing leads should be made safe behind the equipment.
- Liquids must not be taken near the computers.
- Magnets must be kept away from all equipment.

E-Safety in School

E-Safety depends on effective practice at a number oflevels:

- Responsible use of technologies by all staff, pupils and governors; encouraged by the curriculum and made explicit through published policies.
- Sound implementation of the E-safety/Acceptable Use Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems.

School E-safety/AU Policy

Why Internet use is important.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not, and will be given clear objectives for Internet use, using the SMART rules (See Appendix 2).
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content:

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported designated safety lead.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy.

When will children have direct access to the Internet?

- Online content (e.g., CBeebies) will often be used by the teachers for specific tasks (see Appendix 1 for examples of Teaching and Learning Activities). In these situations, the children are not searching the internet or navigating away from the page/s and tasks that have been set. Teachers will have spent a reasonable length of time previewing the site to ensure that it matches the learning outcomes of the lesson/setting.
- Searchable cached sites such as Discovery Education will allow access within a site, but not beyond it.
- Children from Year 5 onwards may use a safe search engine when searching for information. This is not a failsafe way of preventing access to inappropriate sites, but is a good line of defence. Searches will only be permitted when a member of staff is present. Where possible, teachers should have pre-searched for the topic in hand and previewed the hits that will be used based on the fact that search engines do not necessarily give the most appropriate site at the top of their lists.
- In most cases, to avoid fruitless hours of browsing, key website/s will be identified by the teacher for the children to use to find information.
- Searches for images via google, yahoo etc. are not blocked and should be monitored.

Managing Internet Access

Information system security:

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly by OneIT.
- The school uses broadband with an effective firewall and filters. A smooth wall is incorporated into the network which is managed by OneIT.

Use of Email:

Children:

- Children may be given a School email Office 365 account. The account is set up using the school email system, and the school will determine the limitations upon this account. For example a child may have email set up to only communicate within school.
- The children are at liberty to use their accounts for correspondence between one another or members of staff.

Passwords are generated. (children will be issued one to use throughout the year and then it will be changed by staff if it is compromised) and a copy will be stored by the class teacher/Computing Leader. Users agree through the home/school or staff agreement form to keep passwords secret, even from their family and friends. School reserves the right to limit access to this account, at any time.

School has identified that at this stage there is a need for individual 'log-ins' for younger children, and that our children will be expected to maintain the security required with individual passwords given parental or carer assistance. If inappropriate use is found, then it will be withdrawn and the School will investigate alternative forms of providing access.

The email system has a spam filtering system. The email system has no formal method of detecting inappropriate material; therefore before giving out accounts children and parents are made aware of this. As there is no filtering security the administrator/Computing Leader/Head Teacher has the right to access any email account if they suspect abuse of the system. All children are made aware through their home/school agreement statements (given out when they are given an account) that such a filter exists.

Suspicion of offending/abusive emails will be opened and assessed as to the reason why it has been intercepted, for example:

- Offensive language
- Bullying and threatening behaviour

Children will also be expected to report any offensive emails that they receive to a member of staff. Any reports of offensive emails will then be reported to the Head Teacher. Children must also report any attempts by people who they don't know trying to contact them. Children will be taught to never give out their email address in a public setting (virtual or real) or divulge personal details in public internet space in Year 4. This will be reinforced whenever the Internet is used through continued verbal reference and visual reminders.

The use of personal email accounts by children in school, or on equipment issued by School, is not permitted.

Use of newsgroups or forums/chatrooms by children in school is not permitted unless deemed to be for an education purpose by the Computing Leader/Head Teacher.

All of the above information is found in the home/school agreement, which must be agreed, by both the parent/guardian and the child before a user account is allocated. Failure to adhere to the agreement will result in the sanctions contained in the document.

Staff

Staff will be given a "professional" email account. The account is set up using Office 365 . The staff are at liberty to use their accounts for correspondence between one another, other professional bodies as part of their work or appropriate individual correspondence. Staff can use their professional email account for personal use. The staff are all aware that incoming and outgoing emails are monitored and that the administrator has the right under the guidance from the Head Teacher to access accounts at anytime with due reason.

Any digital communication between staff and pupils/parents must be carried out using professional school accounts, all of which must be professional in tone and content. Personal email addresses, text messaging, personal mobile phones must not be used for these communications. Professional email accounts are essential in communicating with a wide range of people, such as staff, parents (reports) and children (relating to class work).

Staff are allowed to access their personal email accounts using school IT equipment occasionally in school. Although personal emails should not be opened in the presence of children, or during allocated or direct teaching time.

The email system has a spam-filtering box; staff are aware of this and understand that it is their responsibility to check this mail before opening them, to help prevent viruses entering the school network. All emails highlighted, which cause a concern to the administrator will be opened and assessed as to the reason why it has been intercepted, for example:

- Offensive language
- Bullying and threatening behaviour

Users will also be expected to report any offensive emails that they receive to the Computing Leader, who will log the incident and report the offensive emails to the Head Teacher (see Appendix 7 for details on reporting incidences). Users must also report any attempts by people who they don't know trying to contact them. Use of newsgroups or chatrooms in school for personal use is not permitted, although it can be permitted for some educational purposes when it is located on the learning platform and with prior arrangement with the Computing Leader or Head Teacher.

The user must change their email passwords. Passwords are not kept in school, ONEIT have the overall authority to change/amend users details under specific guidance from the Computing Leader or the Head Teacher. Users agree through the staff agreement form to keep passwords secret, even from their family and friends.

The staff acceptable use policy sets out the terms and conditions that they must agree to before being allocated an account. This happens in the new staff member's induction meeting. Failure to adhere to the agreement will result in appropriate disciplinary action.

Use of the Photocopier

Staff are required to print via the office photocopier, the data is transferred using the curriculum network. Teachers are required to input their unique year group ID code to access the printer. The printer default settings are sent to a 'custom box', this ensures that all printing is collected and the waste is reduced. Staff are required to input a their name and the code, thiswill help staff identify their own printing when at the machine. The printing will be held in the photocopiers memory until the staff access this at the photocopier. The memory automatically clears in items for not printed within three days.

Digital Images/Videos

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or down- loaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain on the Internet forever and may cause harm or embarrassment to individuals in the short/longterm.

All parents have signed Ormesby Primary Biannual Consent (Appendix 5). Outlining how Ormesby Primary will use images and videos of children. All images must be taken using a school issued device, not a personal device such as a mobile phone.

The images must be wiped clean from the device and stored in a secure password protected environment within 72 hours. It is the responsibility of the adult in charge of any party to checkfor image consent and to ensure that pupils are appropriately dressed and are not participatingin activities that might bring the individuals/school into disrepute. Images can be in many forms:

- Voice
- Photograph
- Video

When using digital images staff should make children aware of the risks associated with taking,sharing, publishing and distributing images. In particular they should recognise the risksattached to publishing their own images on the Internet, especially on social networking sites.

Use of Online Storage Space

Children have their own workspace online. They will be given this after agreeing to the terms and conditions in the home/school agreement. The children will use their space for storing of files and organising information. Inappropriate materials or text found on online will result in removal of access, and the School Code of Conduct/ Behaviour Management Policy will be followed.

At Ormesby Primary School our definition of inappropriate materials include those which encourage race hate, bullying, violence, pornographic material, are illegal or are not an appropriate use of the online workspace, such as personal MP3 collections. The children will be taught how to use this space to create a portfolio of their work and links to/copies of re- sources that they use to complete their school work. Personal files should be stored elsewhere.

Administrators reserve the right to access personal online space when requested by the Head Teacher in writing. Failure to observe this will result in appropriate action by the Head Teacher.

Managing Filtering

The school will work in partnership with the service provider, currently OneIT, to ensure filtering systems are as effective as possible. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the schoolDesignated Safeguarding Lead. OneIT will ensure that checks are made to ensure that the filtering methods selected areappropriate, effective and reasonable.

ManagingEmerging Technologies including Mobile Phones

Emerging technologies will be examined for educational benefit and a risk assessment will be carriedout before use in school is allowed.

- Mobile phones will not be used on the school grounds by pupils at Ormesby Primary. The sending of abusive or inappropriate text messages on school grounds is forbidden and will be reported to parents and the Head Teacher.
- If a mobile phone is brought onto the school premises, it will be handed in immediately on arrival to the school office for safekeeping and collected on the way out of school at 3'o'clock. It will not be stored in bags or pockets. Failure to observe these rules will lead to confiscation.
- Staff will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by mobile phone unless urgent contact is required and for school business, e.g. an emergency with their child on a school trip.
- The wearing of Smart watches will not be permitted in school as they enable access to applications and text/email messages.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- All access to personal data will be password protected.

Published Content and the School Website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

- Pupils' names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing

- Social networking sites and newsgroups will be blocked for pupils, unless a specific use is approved.
- Pupils are taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. (See Appendix 2 - The SMART Rules).
- Pupils and parents will be advised that the use of social network spaces outside school maybe inappropriate for primary aged pupils as many have age restrictions.

Policy Decisions

Authorising Internetaccess:

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the E-Safety/ Acceptable User Policy (AUP) before using any school ICT resource (See Appendix 3).
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy (See Appendices 4 and 5).

Assessing Risks:

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The Head Teacher will ensure that the E-Safety/AUP Policy is implemented and compliance with the policy monitored.

Handling E-Safety Complaints:

- Complaints of Internet misuse involving the pupils will be dealt with by a senior member of staff. Sanctions resulting may include interview/counselling by class teacher / Head Teacher; informing parents or carers; removal of Internet or computer access for a period of time.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communityuse oftheInternet:

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Use of Mobile Devices

Staff mobile phones are permitted within school. It is expected that mobile phones should be switched to 'silent mode' during contact time with children, and they should not be used to make or receive phone calls or text messages during teaching hours. Emergency/important calls should go through the office unless another agreement has been reached with the Head Teacher. Failure to observe this will result in appropriate action by the Head Teacher. Permission is granted for staff to receive their professional emails through their personal phones only if their phone is password protected.

Children's mobile phones are not permitted within school unless the Head Teacher has granted specific permission. They must be handed to staff for storage. Failure to observe this will resultin confiscation. Failure to observe this will result in appropriate action by the Head Teacher.

Devices issued by School, which may have a phone facility are allowed in School, but the phone element must be switched off from 08.55am-3.10pm. Attempts to make or receive phone calls or text messages will result in confiscation. Failure to observe this will result in appropriate action by the Head Teacher. Devices issued to staff, by school, are allowed to access their professional email accounts through them, as long as the device has a secure password. When the device is loaned or used by children this access to emails needs to be disabled.

Devices issued by school will connect to the Internet through the school's filtered broadband connection or via the 3G/4G/ 5G network. Children are allowed to connect their devices to other wireless providers either at home or in the community subject to them following the guidancegiven by school. Any attempts to access children's iPads, for example via Bluetooth, should be reported by a child to a member of staff, who will inform the Computing subject leader. At thatpoint a risk assessment will be done and steps taken to ensure that the iPad/ is not left vulnerable to attack.

Children are at liberty to install software on their devices after approval from the Computing leader. Any software found to be inappropriate or not approved by the Computing leader will be deleted. Failure to observe this will result in appropriate action by the Head Teacher.

When children/adults are using iPads/cameras in school and any other digital device they mustask permission to take any digital image of another person. Failure to adhere to the agreement will result in appropriate action taken by the Head Teacher or Computing Leader.

Parents who have concerns or queries about use of the iPads can contact the Computing subject leader by appointment, who will assess whether the Head Teacher needs to become involved. Steps will be taken to resolve issues where appropriate and lessons learned/implemented where relevant.

Content on school issued mobile phones will be filtered including a 'content control system' toblock adult content via the phone network e.g. SMS MMS Services, and the 4G internet devices for children will only have access to a limited range of services or places via the School broad- band connection.

Dangers

The School states its policy towards the dangers potentially involved in the use of mobile learning and devices below:

Physical Danger:

There is a risk that whilst online, a child may make inappropriate 'friends', perhaps providing information or arranging a meeting that could risk his or her safety or the safety of others. This is perhaps the most worrying and extreme risk associated with Internet use. With the mobile Internet, these risks can potentially be greater. As mobile phones/tablets are such personal andprivate devices it will be difficult for parents to supervise access and contacts in the same way as they would a PC in the home. Mobile phones/mobile devices are typically always on and hence a child is always contactable, and always vulnerable. The rich content capabilities of 4G phones means that young people may be sent inappropriate images or videos, or be encouraged to send back images or videos of themselves using integrated cameras. The integration of cameras within mobile phones/mobile devices may also result in digital images of children andyoung people being taken and circulated or posted on websites without their knowledge or permission. Therefore children are educated in school to ensure they ask per- mission of the person they are taking an image of before proceeding. Children are also taught about the level of information, which should be shared on line and the dangers of this.

Services may also provide more opportunities for personal contact, for example by SMS (short message service) or MMS (multimedia message service) chat, online gaming or dating services . Additionally, location-based capabilities may mean that it is possible to pinpoint the exact location of children and young people. Whilst this may be welcomed by parents keen to know where their child is at all times, it is not difficult to see how misuse of the technology could arise.

Parents will therefore have access to training in school to address these issues. It will be the parent's responsibility to attend.

School will explain to pupils the possibility of the attempted/ actual theft of the device. Devices will be security marked. School will inform the Police of the allocation and distribution of equipment into the local area. Children will be expected to 'pocket or bag' the device whilst travelling to and from School; they will be given guidance on safe use and storage, both at home and travelling to and from School.

Cyber Bullying:

Cyber bullying, for example by text message, email or via websites is a growing concern associated with the fixed Internet and mobile telephone use. The mobile Internet may unfortunately offer a further way for bullies to torment their victims. Such behaviour will be dealt with following School procedures. (Please see our Cyber Bullying Policy).

Sexting:

When responding to and managing incidents of sexting, we refer to the 'UK Safer Internet Centre' (SWGFL) guidelines and school online safety policies.

Communications Policy

Introducing the E-safety/Acceptable User Policy to pupils:

- Rules for Internet access will be posted in all networked rooms – The SMART poster (See Appendix 2).
- The poster will become the wallpaper for log on screens as a regular reminder of the rules.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use (See Appendix 1 for examples of Teaching and Learning Activities).

Staff and the E-Safety/ AU Policy

- All staff will be given the School E-Safety/Acceptable User Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be given a "professional" email account.
- The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work.
- Passwords must be changed by the user who agrees, through the staff agreement form, to keep passwords secret, even from their colleagues, family and friends.
- Users will also be expected to report any offensive emails that they receive to the head teacher. Any reports of offensive emails will be reported to the Head teacher. Users should also report any attempts by people who they don't know trying to contact them.
- School professional email accounts should not be used for personal communications; use is dedicated to educational matters only.
- Use of newsgroups or forums/chat rooms in school is not permitted unless located on the school network.
- The staff internet agreement form sets out the terms and conditions that they must agree to before being allocated an account. Failure to adhere to the agreement will result in referral to the Head teacher and possible disciplinary action (See Appendix 3).

Enlisting Parents'/Carers'Support:

- Parents' / carers' attention will be drawn to the School E-Safety/Acceptable User Policy upon joining the school and if significant amendments are made.
- A school document 'A Parents' Guide to Video Games and Online Safety' will be issued to all new parents in school and be accessible through the school website (See Appendix 6).
- School, through the Head Teacher or Deputy Head Teacher, will contact parents where concerns have been raised about a pupil's access to age-inappropriate games, DVDs etc.

Signed Agreement:

- Parents will be asked to sign the policy agreement on behalf of their children upon enrolment in the school. The agreements will be stored in a file in the school office until the child leaves.
- Staff will be asked to sign the agreement upon joining the school. These will be updated when significant changes are made to the policy. The signed agreements will be stored in a file in the school office.

Reporting Incidents

A very important element of safeguarding is the ability to identify and deal with incidents. All staff and pupils have a responsibility to report online safety incidents, so that they may be dealtwith effectively. All incidents should be reported using the CPOMS system under the correct heading.

Incidents must include the correct members of the online safety team and be action appropriately in order to generate a chronology on this new platform. Incidents will be dealt with in accordance with school policies.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key E-Safety Issues	Relevant Websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material theyare uncomfortable with.	Safe Search for Kids Ask Jeeves for kids CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts under direct supervision. All communication must be approved by an adult.Pupils should never give out personal information.	E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal informationshould be omitted.	School website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupilsto be identified. File names should not refer to the pupil by name.	School website
Communicating ideas within chat rooms or online forums.	Only selected chat rooms dedicated to educational use and that are monitored directly by an adult should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	With adult approval
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password shouldbe used.	

Appendix 2: Internet use - The SMART Rules

Appendix 3:

Ormesby Primary Staff and Governor

Technology Acceptable Use Agreement / Code of Conduct

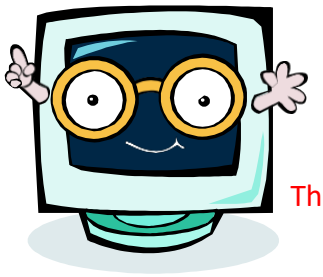
ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure thatall staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's hardware / email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by theschool or other related authorities.
- I will ensure that all electronic communications are compatible with my professionalrole.
- I will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by personal mobile phone unless urgent contact is required and for school business, e.g. an emergencywith their child on a school trip.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address,to pupils.
- I will only use the approved, secure e-mail system for any schoolbusiness.
- I will ensure that personal data (such as data held on MIS (Sims) software) is kept secure and is usedappropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- Images of pupils and or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent/carer. Images will not be distributed outside theschool 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 loggedand can be made available, on request, to the Headteacher. I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety (including data security) policy and help pupils to besafe and responsible in their use of ICT and relatedtechnologies.

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

Signature …… Date ……..

Full Name ……(printed



Ormesby Primary

SMART Rules for ResponsibleUse of Technology

The school has installed computers and Internet access to help our learning.
These rules will keep everyone safe and help us to be fair to others.

- ☐ I will only use school computers for school work.
- ☐ I will only use the internet when my teacher has given me permission.
- ☐ I will always be polite when using the internet or email.
- ☐ I will not download files or bring in disks or USB memory sticks from outside the school unless I have been given permission.
- ☐ I will NEVER give out my address or telephone number to any other internet user.
- ☐ I will only send email that my teacher has approved so that they can be sure I am kept safe.
- ☐ If I am uncomfortable or upset by anything I discover on the internet, I will report it to an adult immediately.
- ☐ I will only use search engines that my teacher has approved.
- ☐ I understand that if I fail to keep these rules, I will not be allowed to use the internet in school.

Appendix 5

ICT Acceptable Use Agreement for Primary Pupils

At Ormesby Primary, pupils are expected to:

- Only use ICT on the school premises for studying purposes.
- Make sure ICT communication with other pupils and adults is polite and responsible.
- Be responsible for their behaviour while using ICT.
- Inform their class teacher of anything they see online which makes them feel uncomfortable.
- Understand that their use of ICT can be checked and that parents/carers will be contacted if a member
  of school staff is concerned about a pupil's e-safety.
- Be careful when using computer equipment and treat it with respect.
- Abide by the rules regarding bringing personal devices into school.
- Seek the advice of a teacher before downloading material.

Pupils will not:

- Try to bypass the internet settings and filtering system.
- Share passwords.
- Delete or open other people's files and documents.
- Use other people's accounts.
- Send any content which is unpleasant. If something like this is found, such as inappropriate images or the use of offensivelanguage, pupils will report it to their teacher.
- Share details of their name, phone number or address.
- Meet someone they have contacted online, unless it is part of a school project and/or a responsible adult is present.
- Upload images, sound, video or text content that could upset pupils, staff and others.
- Try to install software onto the school network.

Parents will:

- Support and uphold the school's rules regarding the use of school ICT systems.
- Understand the school is not liable for any damages arising from use of IT equipment and systems.
- Act in accordance with the school's policy when using the internet in relation to the school, itsemployees and pupils.
- Only store and use images of pupils for school or private purposes, acting in line with the school's ITPolicy, and not share images of other pupils on-line.
- Understand that whilst the academy uses a combination of filtering and supervision to manage access to the internet and IT systems, that the academy can't be held responsible for children accessing inappropriate materials/the nature of all the contenthosted on the internet.

Ormesby Primary School Parental Consent

Name of parent/ carer completing this form	
Name of pupil:	
Year Group:	

Declaration

I,_____(name of parent), understand:

- Why my consent is required.
- The reasons why Ormesby Primary School uses images and videos of my child.
- Which other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with myrequirements.
- The reasons why Ormesby Primary School sends me marketing material.
- Which other organisations may send me marketing material.
- The conditions under which the school will send me marketing material.
- I have provided my consent above as appropriate, and the school will send marketing material in line with my requirements.
- Consent is refreshed on a bi-annual basis.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the Head Teacher.

Name of parent:_____

Signature: _____

Date: _____

If you have any questions regarding this form, please do not hesitate to contact the Head Teacher at School.

Providing your consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

I provide consent to:	Yes	No
Using images of my child on the school website.		
Using videos of my child on the school website.		
Using images of my child on social media, including the following: • Twitter, Facebook		
Using videos of my child on social media, including the following: • Twitter, Facebook		
The local media using images of my child to publicise school events and activities (only including the organisations outlined above).		
The local media using videos of my child to publicise school events and activities (only including theorganisations outlined above).		
Using images of my child in marketing material, e.g. the school brochure and prospectus.		
Sharing my child's data with a school-appointed external photography company for official school images. Thisincludes the following: • Name, Class, Roll number		

I provide consent to:	Yes	No
Receiving marketing material via email.		
Receiving marketing material in printed copy.		
Receiving marketing material from the following organisations within the school: • The PTA, The Governing Body, The Leadership Team		
Receiving marketing material from the third-party organisations, judged appropriate by the Head Teacher		
Receiving marketing material via email from third parties.		
Receiving marketing material in printed copy from third parties.		
Receiving marketing material for the academic year 2018/19 and 2019/20		

I provide consent to:	Yes	No
Allow my child to use School and Cloud based systems to support learning, including email.		
Allow my child to access the internet to support learning.		

Ormesby Primary

Parents' Guide to Video and Online Safety.

Setting up parental controls.

Besides checking PEGI ratings to help choose suitable games, parents can activate parental controls. This is much easier than it sounds and links to instructions can be found on our school website 'Parents' pages for many of the latest generation of gameconsoles - including Xbox 360, Wii U™, Sony Playstation 3 and PSP, Apple and PC controls.

Using these controls, you can restrict the rating or level of contentthat your child can play, and in some cases who your child plays with online and for how much time.

Parental controls ensure that your child has a fun and secure gaming experience.

Making sure your child's video game experience is safe and secure.

At Ormesby Primary, we ensure that the children know how to keep themselves safe online and what to do if they feel uncomfortable about any content they might see.

The children also learn how to behave responsibly online both at homeand at school in order to make everyone's online and gaming experience a good one.

A guide for parents about choosing age-appropriate games,setting up parental controls,and making sure yourchild'svideogameexperience issafeand secure.

Video games are a great source of learning and entertainment, but it is important for parents to appreciate what playing games today involves inorder to keep their children safe.

A large number of games can be played over an internet connection. Being aware of the tools at a parent's disposal are crucial to ensure that children are safeguarded from inappropriate content and encounters withother players.

Some widely available video games contain graphic violence, virtual sex, violent and gory scenes, partial or full nudity, drug use, portrayal of criminal behaviour or other provocative and sensitive material.Online gaming platforms often offer text chat, the use of headsets or even video for live communication with other players. Unfortunately, the anonymity of online gaming seems to encourage some players to post obscenitiesand unsuitable material which are difficult to control.

Guide to Video Game Ratings

It is probably true that most parents have grown up with the video or DVD classification system. However, this is not always the case with videogames. All too often, the child is more adept at using the computer or games consoles and parents do not know how to access what he or she is playing. As a result, it is important to have something to guide parents when making a decision about whether a game is suitable or not.

The PEGI System (Pan-European Game Information)

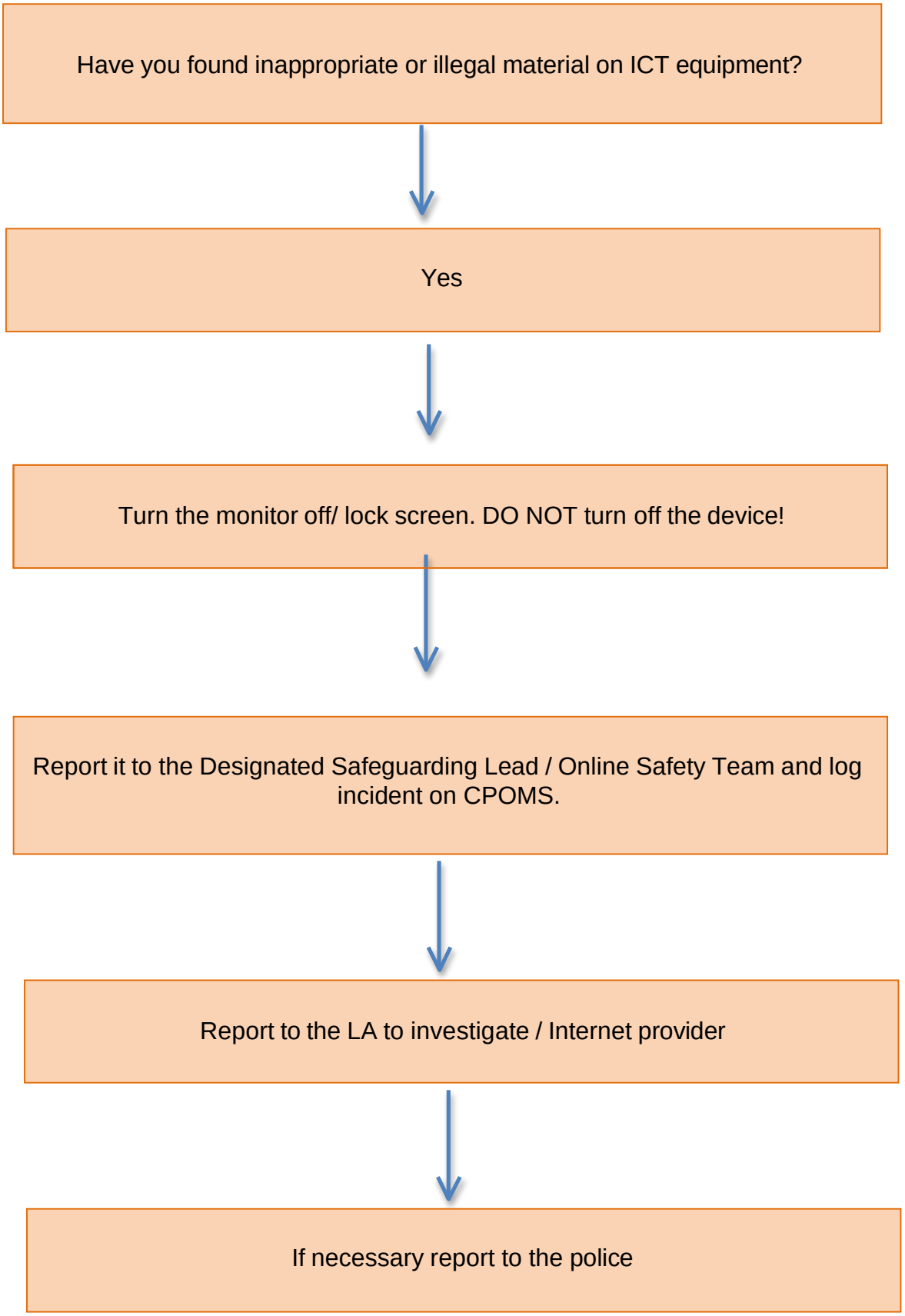
From the summer of 2012, the PEGI system has been used by UK law for age rating video games. The age ratings 12, 16 and 18 are mandatoryand it is illegal for a retailer to supply any game to someone below the age specified.

It is important to note that the age ratings relate to the content of the game and not how difficult it is to play. So, for example, a chess game would be too difficult to give to a 3 year old but it will have a '3' rating as the content is inoffensive. Likewise, a game which is easy enough for a10 year old to play will be given an '18' rating if the subject matter or content is only suitable for adults. Therefore, a '3' or '7' rating does not mean that the game will be too easy for your child but that the content is suitable for primary age children.

Descriptors shown on the back of the packaging indicate the main reasons why a game has received a particular age rating. There are eight descriptors: violence, bad language, fear, drugs, sexual, discrimination, gambling and online gameplay with other people.

Further information on the PEGI ratings can be found at : http:ffwww.pegi.infofenfindexfidf33f

Appendix 7a: Responding to incidents of misuse/error



Appendix 7b: Responding to incidents of misuse/error

Dear Staff,

As you are all aware we have a walled garden in school, which filters the websites which you and the children are al-lowed to access, for safety reasons. This system in not 100% guaranteed therefore we need to be aware of potential risks, for both children and adults.

There are procedures set out in the Online Safety policies in school to follow if such events arise. These are summarized below.

You need to:

- Immediately turn the screen off / put the device to sleep (pressing home/lock button)
- Leave the website on the computer/ device
- Report it to the Online Safety Team /HT immediately
- Log incident on CPOMS with required action and including appropriate staff
- If required It will be investigated by our Internet provider
- If needs be then it will report to the police.

Just remember it is not yours or the children's fault, but it does need dealing with!

This proceed should be followed and children in all classes should be made aware of it.

Appendix 7c: Responding to incidents of misuse/error

Misuse of the Online Safety Policy

If you find you or another member of staff have possibly not abided by the Online Safety policy and rules have been breached, then please follow the following procedures to rectifythe problem.

Seek advice from the Online Safety Team
(Who will if necessary have an unofficial word with the Head Teacher)

Word of advice (reminder if it continues)

CONTINUAL ABUSE 

Computing Leader will refer the matter to the Head Teacher

A meeting will take place with the Head Teacher and Computing Leader.
Minutes of the meeting taken and monitored

Formal investigation into continual abuse of the school policy

CONTINUAL ABUSE 

LA will be informed and disciplinary proceedings will commence