Overfields Primary School

Ironstone Academy Trust

Computing & Online Safety

Updated: May 2022
Review July 2024
IAT Author: Carl Faulkner,
Sonia Herlingshaw

At Overfields 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.

All parents are required to read all the policies linked to the use of technology with their children. They are then required to complete the forms in appendices 8-10. If these are not completed and returned to school, access to technology will be limited for safety reasons, e.g., Internet etc.

Contents **Page**

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 practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, 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 (Early Years Foundation Stage) 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 years learning 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 help children to develop their communication skills.

ELG (early learning goals) for the End of the Reception Year:

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

At the end of key stage 1 pupils should be taught to:

- understand what algorithms are, how they are implemented as programs on digital devices, 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 or contact on the internet or other online technologies

By the end of key stage 2 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 detect and 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 for communication 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 range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behavior; identify a range of ways to report concerns about content and contact

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 lead and 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.

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 adapt the 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 Overfields Primary School we 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 information 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 inthe 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 a la contractor every five years and all port- able 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 into school but if this is necessary, then the equipment must be pat tested before being used in school. This also appliesto any equipment brought into school by, for example, people running workshops, activities, etc. and it is the responsibility of the member of staff organizing 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, SBM 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

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 wellas develop computing.

Parental involvement
Parents are encouraged to support the implementation of computing where possible by encouraging use of computing skills at home during home-learning tasks and through the school website. They will be made aware of online safety links and encouraged to promote thisat home. We will create opportunities for parents to develop their knowledge in this field further with annual online safety training and drop-in sessions. 'Marvellous me' is an app usedto consolidate learning, encourage and praise children and engage parents with their child's learning journey. This has been successfully rolled out across school and is a direct line of communication with parents.

Social Networking
The widespread availability and use of social media applications brings opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. (Please see Social Networking Policy).

Twitter
At Overfields Primary School we use twitter as a tool to communicate with the world around us and craft our professional online identity. As ultimately anyone has the potential to create our online identity, we, as a school, want to manage our own online presence. Our school has a twitter account and staff are encouraged to use this. The account is to be sanctioned by the Head teacher and monitored regularly. Tweets reflect our school policies.
It is the account holder's professional responsibility not to approve tweets that would be deemed 'derogatory' for our school. Photo permissions are obtained for every child upon entry to school.

Code of conduct for staff

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation and GDPR (General Data Protection Regulations UK) Compliance.

Staff are to ensure they sign the AUP (Acceptable Use Policies) in which we identify acceptable behaviours for personal accounts. (Appendix 6 & 6a)

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses

phone numbers and other personal information. Staff must use a separate email address just for social networking so that any other contact details are not given away.

Facebook is targeted at older teenagers and adults. They have a no under 13 registration policyand recommend parental guidance for 13-to-16-year Olds. The following are extracts from Facebook privacy policy:

"If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information froma child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us"

"We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices."

As a school we educate our parents and children about the dangers surrounding social networking sites.

You Tube

Overfields Primary School has its own professional YouTube account which is set to private. Allvideos uploaded must be set to 'unlisted' in which the URL can be distributed in order to see the clip. The video will be uploaded for professional use only. For example, in conjunction with awards we have won (Naace 3rd Millennium Learning Award) to help leading other schools in their professional development and to raise the profile of our school. If pupils feature in these videos consent would have been approved by the parents or carers by the signing of the digitalmedia consent document upon entry to school.

Mobile Device Management (MDM)

Our school uses 'Zuludesk' MDM to effectively manage the profiles on our devices. The profile allocates app codes bought through the volume purchasing and distributes accordingly. Restrictions are also placed on the devices managed as a further level of security.

Online Safety

Our school internet policy was created by the Head teacher and Computing leader. It has been discussed by the whole staff and approved by governors, who realise how intrinsic to the running of the school, both at a management level and an educational level, the Internet is.

The Internet is now the most data rich source of information in the world. It can potentially "bring the world into the classroom." From a teaching point of view this is an essential resource for planning and delivering lessons. From a child's point of view, it is an excellent source of information that enhances the personalised learning agenda.

This policy seeks to ensure users know what good practice is and outlines steps and procedures that will be taken when the darker side of the Internet shows itself.

Roles and Responsibilities

Headteacher Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the OFSTED accredited Online Safety Lead and the Online Safety Team.

The Head teacher and Senior Leadership team will ensure that the online safety and relevant members of staff receive suitable training to enable them to carry out their role and to train other colleagues as relevant. The Senior Leadership Team will ask for regular updates and monitoring reports from the Online Safety Team.

Online Safety Governor

Mr A Simpson is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of this policy. This will be carried out by the Governors, and they will be receiving information about incidents and monitoring reports. Their role includes:

- meeting with the Online Safety Lead
- regular monitoring of Online Safety incident logs
- monitoring of filtering
- reporting to the relevant Governors

Online Safety Lead

Mrs. C Guilfoyle

Her role is:

- to lead the Online Safety Team

Mrs Watson	Headteacher/ Designated Safeguarding Lead
Mrs C guilfoyle	School Online Safety Lead
Mr. Simpson	Online Safety Lead Governor

- takes day to day responsibility for safety issues and has a leading role in establishing and reviewing the Online Safety Policy / Documents
- ensures all staff are aware of procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with local authority and other relevant bodies
- liaises with school technical staff
- receives reports of online safety incidents
- meets with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings
- Report to Senior Leadership Team

Filtering

The school's 100MB broadband connection is provided by Aspire/ OneIT, which in turn links into the Smoothwall. The web filtering solution Smoothwall is compliant with the government's Prevent Strategy. Smoothwall are a leading UK filtering provider. The filters at each stage are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows direct access and sharing of resources between educational establishments. However, when dealing with the Internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken.

We therefore aim to educate them about online safety, not simply cover their eyes.

Data Security

Data is stored in numerous places in school depending on the sensitivity of the information. The level of access is determined in the table below.

Level of security	Type of Data	Accessible by whom…
Restricted Data - personal information related to staff and pupils	SIMS CPOMS	Teachers Office staff HT
Password protected. Only staff, Year 4 Year 5 and Year 6 children have access to this.	Email	Staff Selected children (Year 4, Year 5 and Year 6)
Password protected. Only staff, pupils etc.	School – Purple Mash Logins Names and	Parents Children

Names collected in SIMs are given passwords. Parents of the children are allowed to use these alongside their children	Photographs Timestable Rockstars Spelling Frame Oxford Owl	Staff (People who are given a password by Computing Leader)
None	School Website	All
None	School Twitter	All

Teachers are expected to use a diverse range of technology and software packages for a range of teaching and non-teaching tasks. Teachers are expected to use SIMs and CPOMS (an electronic storage area, storing personal data on children and staff) to take the register, log incidents, store reports and input performance data.

Internet access

The school has provided enhanced user-level filtering through the use of the school filtering system; this allows teachers to view more web sites than children. For example, shopping webpages have been unblocked to allow teachers to purchase resources for school.

The decision was made by the Headteacher and the Computing Leader to give different users different levels of access to web pages. The sole purpose of this was to allow teachers the abilityto search web pages for resources that would not necessarily be appropriate for children, for example YouTube. (See appendix 2a & 2b, levels of access clarified)

Children in all classes in school will have access to the Internet. However, the different types ofuse are outlined below:

- Online content will often be used by the teachers for specific tasks. In these situations, thechildren are not searching the Internet or navigating away from the page/s and tasks that have been set. Teachers ***will have previewed the site*** to ensure that it matches the learning outcomes of the lesson/setting. With younger children it is essential where possible that access to navigate away accidentally is denied (i.e., hiding the address bar). The importance of being safe on the Internet will be discussed prior to using theInternet. The consequences of navigating away from the preferred web page will be discussed with the children.

- Children from Year Two onwards will use a search engine such as Bing / Kidrex when searching for information. This is not a failsafe way of preventing access to inappropriate sites, but it 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 thetopic 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, a key website/s will be identified by the teacher for the children to use to find information. This can be made easier with the use of bookmarks.

- Year 5 and 6 will be taught to take ownership and understand the importance of information, which will have a positive impact on their learning. Therefore, searching on the Internet may be appropriate, but must be carried out in the presence of a member of staff.

Children will not be allowed to access and search the Internet unless authorised by a member of staff.

Teachers are allowed to use chat rooms / webinars as part of their work although these must be checked prior. Teachers must understand that these web sites are not regulated and therefore only non-identifiable information is posted on there. Avatars should always be used when they are used with pupils. Blogs and forums can also be used by staff, to support their work with an educational focus, e.g., twitter.

Staff and children are permitted to use online storage space, such as Google docs, iCloud and One drive. These allow the staff and children to share documents wherever they are.

Responsibility for the monitoring of what the children find is then the responsibility of that adult. The school 'Scheme of Work' and 'Non-negotiables' for Computing should be referred to, to understand when it is appropriate to search the Internet; other uses are the sole responsibility of the supervising adult. Appropriate behaviour and understanding of how addresses are composed will be explicitly taught before ever using an Internet search in school and will be reinforced by visual reminders.

Accessing the Internet at home

The use of mobile computing devices and connecting to the school's network from home is increasingly important but presents a number of security risks, which need to be addressed. Users of mobile computing facilities (such as laptops, iPads etc.) are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or dam- age of such items and to prevent unauthorised access to information held on the device. Particular care should be taken when leaving devices in cars, hotels, at home, or even in school to ensure they are not visible. Where possible mobile devices should be locked away when not in use.

Staff are allowed to link their school laptops to their home internet, this is to allow staff the facility of email, therefore giving them access to data which could be of a sensitive nature. If staff do not wish to install the Internet on their school laptop at home, the school will assist in the purchase of a 3G dongle.

With technology and ways of communicating advancing rapidly we need to ensure we keep abreast of the advances/changes. As a school we need to ensure our entire 'community', both ex and existing staff and pupils are protected, and privacy rights are not breached. Therefore, text or photographs should not by posted on sites, such as 'Facebook' which have a direct link to school, e.g., school photos, work etc.

The school from time to time to supplement this Policy will publish additional guidance. All employees should assume that it is their responsibility to ensure that there is a separation of their schoolwork and their digital life outside of the workplace.

External Storage Devices

In order to avoid staff carrying sensitive data on laptops/memory sticks, the school agrees toteachers using encrypted memory sticks only as and when required.

Teaching safe use of the Internet

Accessing and interacting with the Internet is part and parcel of many users' reasons for havingan Internet connection. Simply blocking the children from using the Internet does not educate them for the real world (and use at home). Therefore, online safety is implicitly taught in Key Stage 1 and 2 and referred to whenever a unit of work requires use of the Internet.
Key themes to be covered are listed below:

- Safe browsing on the internet
- Use of chat rooms
- Use of social networking
- Use of blogs/webspace
- Use of email
- Copyright
- What to do when you come across something that is inappropriate

The materials and links to resources used to teach these issues are included in the attached appendix (Hectors world/www.thinkuknow.co.uk). Use of the network for personal monetary profit or gambling is strictly forbidden.

Use of email

CHILDREN

Children may be given a School email Office 365 account. The account is set up using the schoolemail 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/HeadTeacher 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 hasbeen 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 mustalso 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 Inter- net 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 deemedto 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, byboth 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.

Use of email

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 any time 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 rangeof 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 occasion- ally 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 theirresponsibility to check this mail before opening it, to help prevent viruses entering the school network.
All emails highlighted, which cause a concern to the administrator will be opened and assessedas 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 flowchart, appendix 3). Users must also report any attempts by people who they don't know tryingto contact them. The use of newsgroups or chatrooms in school for personal use is not per- mitted,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 has the overall authority to change/amend users' details under specific guidance from the Compu- tingLeader or the Head Teacher. Users agree through the staff agreement form to keep passwordssecret, 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 members' induction meeting. Failureto adhere to the agreement will result in appropriate disciplinary action.

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 downloaded 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 remainon the Internet forever and may cause harm or embarrassment to individuals in the short/longterm.

All parents have signed Overfields Primary Biannual Consent. **(Appendix 8)** Outlining how Overfields 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 check for image consent and to ensure that pupils are appropriately dressed and are not participating in 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 risks attached 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 files and organising information. Inappropriate materials or text found online will result in removal of access, and the School Code of Conduct/ Behaviour Management Policy will be followed.

At Overfields Primary School our definition of inappropriate materials includes 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 resources that they use to complete their schoolwork. 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.

Wireless Network security

The school's wireless network is encrypted so as to prevent unauthorised access. It will be checked and authorised by OneIT. If a breach in security is discovered, it will be reported to the Head Teacher / Computing Leader and steps will be taken to review the security level in place with relevant specialists. The wireless network has a minimum security of WPA2 encryption, to prevent any uninvited users, with a further restriction of the firewall.

The Head Teacher / Computing Leader made the decision to give different users different levels of access to the web through the use of different ports. (See appendix 2).

In the event of the network manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged by the Computing Leader and carried out by a process that is agreed by the Head Teacher.

Any requests by staff to open/remove some levels of filtering will need to be considered by the Computing Leader/Head Teacher. If the request is agreed, this action will be recorded and monitored.

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. Per- mission 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 result in 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 guidance given 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 that point a risk assessment will be done, and steps taken to ensure that the iPad/ is not left vulnerable to attack.

Appendix 1 shows how the school currently considers the benefit of using these technologies for education outweighs their risk/disadvantages.

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.

All children will sign an ownership agreement form that sets out the terms and conditions of using the device before receiving the kit (see appendix 5, 5b & 5c).

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 being taken by the Head Teacher or Computing Leader.

Parents who have concerns or queries about use of the iPads can contact the Computing subjectleader 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.

Starters and Leavers

It is the responsibility of the office staff to inform the Computing leader/ Technician of any member of staff/pupils or governors joining or leaving the school. The staff/pupil/governor leaving will have to return all ICT equipment owned by the school to the Computing leader. Thetechnician will then ensure that leavers' access is removed or disabled. All new starters, whether they are staff or pupil will need to have read, understood and signed the school acceptable use policy, before any will be granted access will be granted to any ICT equipment. All visitors requiring access to school ICT equipment need to sign the acceptable use policy. Theschool office supplies all new members of staff, students and supply teachers with the AUP form the read and sign as well as temporary log in details for the school network, only. When the new starter data has been entered into SIMs then a more permanent log in will be issued to staff from the school network. (See appendix 6 & 6b)

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

Other Areas of Teaching and Learning

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 their name and the code; thiswill help staff identify their own printing when at the machine. The printing will be held in the photocopier's memory until the staff access this at the photocopier. The memory automaticallyclears in items for not printed within three days.

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 and private 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 and young 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 online 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 (iMessage). 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 parent's keen to know where their child is at all times, it is not difficult to see how misuse of 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 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 in the 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.

Legal, financial and commercial considerations

With the fixed Internet there are concerns that a child could do something that has legal or financial consequences such as giving out a parent's credit card details or doing something that contravenes another person's rights. Plagiarism and copyright are particular issues, which are associated with the Internet, especially in relation to downloading music or games. Research also shows that children are not able to differentiate between what is advertising and what is not.

Again, all of these issues could potentially increase with the mobile Internet with easy access to chargeable content in the form of games, downloads, ringtones, logos and other services all of which are particularly attractive to children and young people. The facility to pay for goods and services using mobile devices as an 'electronic wallet' is also set to increase. Spam by text message is already a growing problem, and the rich media capabilities of 3G/4G devices will undoubtedly mean that advertisers become more sophisticated in their campaigns. Therefore, children are taught about the issues linked to Plagiarism/copyright and downloading material from the Internet. Children and staff are encouraged to use images, etc., which carry the 'creative commons' symbol. (See appendix 7 for a list of illegal acts).

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

Reducing the risks

The dangers and risks associated with using 4G or mobile Internet services can be reduced through effective education of the safe and appropriate behaviours to adopt when using this new technology.

In common with general online safety recommendations, children and young people should be taught the importance of keeping personal information private, the appropriate behaviours to use when online, the need to critically evaluate any information they find, and the importance of seeking advice from an adult if they see any content or are contacted in a way which makes them feel uncomfortable. Additionally, School will source its mobile learning solutions from a recognised and reputable supplier and network, which will be expected to sign up to and follow best practice, statutory regulation and any relevant Codes of Practice.

Parent involvement

The Head Teacher will offer to meet with parents and carers each year and cover the issuesraised in this Policy.

There will be a yearly meeting, open to parents, carers and Governors with the Child Protection Officer in addition to the above.

The procedure for parents and carers who are not happy with some aspect of ICT use/teaching is the same as with all other concerns.

- Class teacher made aware
- Computing Leader informed
- Head Teacher informed

Parental consent forms will be stored in children's individual files in the Head Teachers office.

T Watson
Head teacher

C Guilfoyle
Computing/ Online Safety Lead

A Simpson
Online Safety Governor

Appendices **Page**

Appendix 1

Communications

Communication Technologies	Staff & other adults				Students/Pupils			
	Allowed	Allowed at a certain time	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✔						✔	
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones/personal devices or other camera devices not owned by school				✔				✔
Taking photos on mobile phones/personal devices or other camera devices owned by school	✔				✔			
Use of handheld devices e.g., iPads/ iPods	✔				✔			
Use of personal email addresses in school, or on school network		✔						✔
Use of school email for personal emails	✔							✔
With e-safety Training and in a professional capacity only…								
Use of chat rooms/facilities		✔					✔	
Use of instant messaging		✔					✔	
Use of social networking sites		✔					✔	
Use of blogs		✔					✔	
Marvellous Me	✔							

Appendix 2

Wireless Network SSID

User
NPS (Normanby Primary School) Staff Wi-Fi
NPS Pupil Wi-Fi
NPS Guest Wi-Fi

Any unauthenticated device internet is heavily filtered however devices can be assigned a static IP (Internet Protocol)address which would all the filtering to be more relaxed.

Any authenticated devices filtering will be based up the authenticated user groups.

Guest SSID is on a separate network which gives the device a 192 IP Address when connecting to the internet users will be asked to log in.

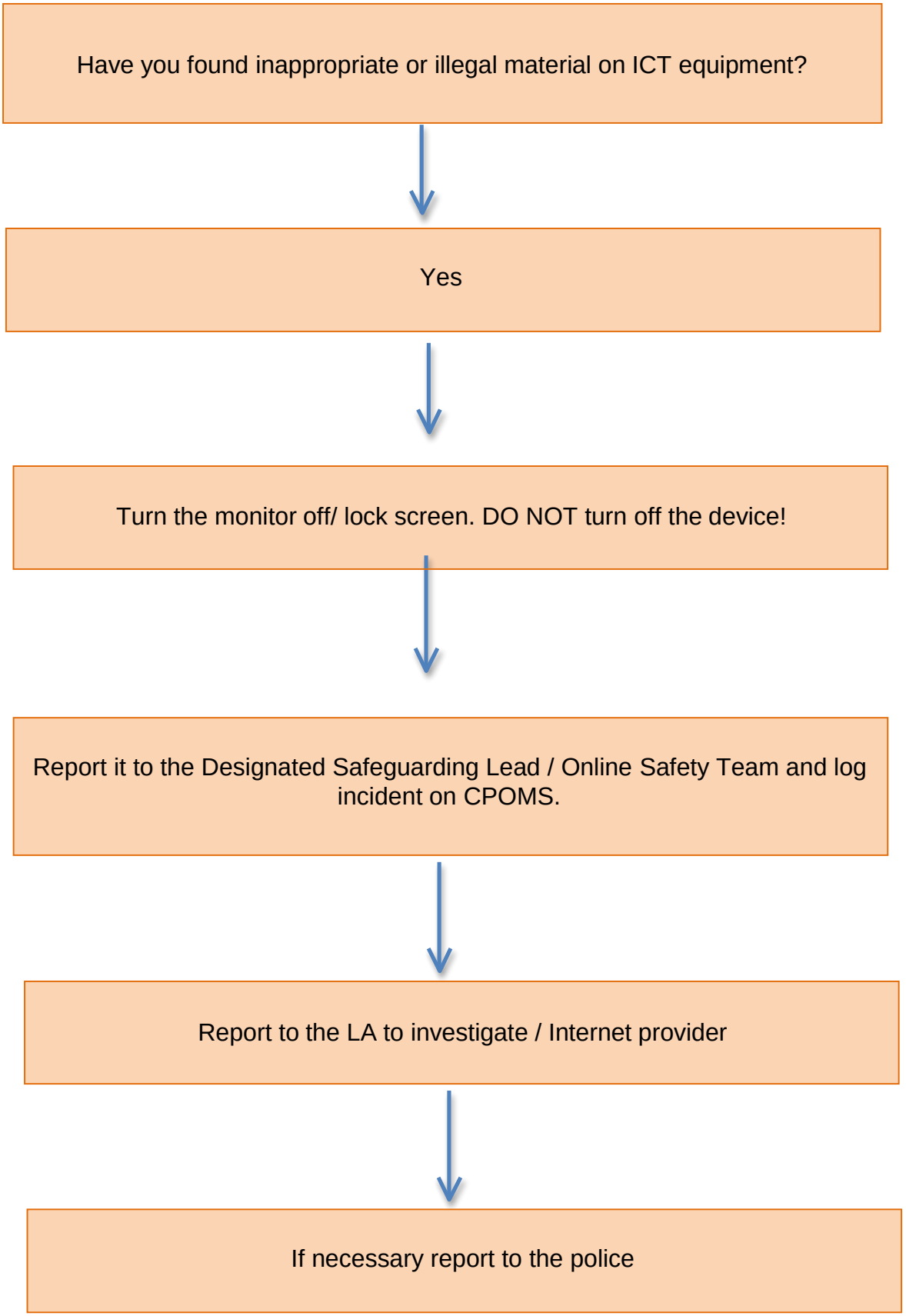
Appendix 2b
User Actions…

Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

	Acceptable	Acceptable at certain times	Acceptable for nomination	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✔
Promotion or conduct of illegal acts					✔
Adult material that potentially breaches the Obscene Publications Act in the UK					✔
Criminally racist material in the UK					✔
Pornography				✔	
Promotion of any kind of discrimination				✔	
Promotion of racial or religious hatred				✔	
Threatening behavior, including promotion of violence or mental harm				✔	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✔	
Using school systems to run a private business				✔	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LA/school				✔	
Uploading, downloading or transmitting commercial software ware or any copyrighted material belonging to third parties, without the necessary licensing permissions				✔	
Revealing or publicising confidential or propriety information				✔	
Creating or propagating computer viruses or other harmful files				✔	
Carrying out sustained or instantaneous high-volume net-work traffic that causes network congestion and hinders others in their use of the Internet				✔	
Online gaming (educational)				✔	
Online gaming (non-educational)				✔	
Online gambling				✔	
On-line shopping/commerce e.g., fruit shop	✔				
File sharing	✔				
Use of social networking sites	✔				
Use of video broadcasting with adult guidance e.g., YouTube	✔				

Appendix 3

Responding to incidents of misuse/error



Appendix 3b

Dear Staff,

As you are all aware we have a walled garden in school, which filters the websites which you and the children are allowed to access, for safety reasons. This system is 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 it needs to be then it will be reported to the police.

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

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

Appendix 4

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 rectify the problem.

Seeking 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 (Local Authority) will be informed, and disciplinary proceedings will commence

Acceptable Use Policy for iPads
School iPad

Your iPad will be linked to the school internet.

Only use websites which you are directed to. (Don't go on inappropriate websites!)
Always ask your parents / carers permission when linking your iPad to your home network as responsibility for home internet use lies with them.
I understand that the school may check my files and monitor the internet sites I visit at school.
Only go on the internet when the teacher asks you.
Always ask permission before taking a photo or video of another person.
Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.
Always ask permission before changing any settings on your iPad.
Charge your iPad every night ready for learning the next day.
Always use the charger it came with.
Bring your iPad to school every day, as it is a vital learning tool.
Make sure you only take videos and photos in an appropriate setting (e.g., not in a bathroom, bedroom etc.)
School is silent! (Turn your volume off in school)
Always remember to take your iPad home at night.
Only ever touch your own iPad. Only touch other devices if you have permission.
Personalise your own iPad, with a screen saver and wallpaper appropriate for school.
Keep all documentation in a safe place at home.
When you are not using your iPad lock it away in a safe place.
Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).
Always send polite and responsible messages, messages will be monitored.
I understand social networking apps or websites are not permitted in school.
I understand school will provide me with some key apps for my learning and I must not delete them. School also provides a more secure network for me to access the internet and other Wi-Fi networks.
Always ask before downloading additional apps and make sure they are age appropriate.
Always ask permission if linking your iPad with a different Apple ID. (Parent or Carers may have detailsthey don't want you to access).
I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionalityat school if teachers deem so.
I understand that my iPad will be linked to schools mobile device manager system, school can see my device and what apps I am downloading and restrict content.
I am clear that school retains the right to restrict any content deemed unsuitable.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn't written above, don't do it!
You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

Child Name:		Parent/ Carer Name:	
Signature:		Parent/Carer Signature	
Date:		Date:	

Pupils, parents, carers, staff and governors all want Normanby Primary to be a safe and happy place, so that you can learn and enjoy your time at school. All of our policies reflect this, and we all should use anyitem of equipment in a sensible, kind and thoughtful manner.

Normanby Primary School

Acceptable Use Policy for iPads
Home iPad

- I understand at school my iPad will be linked to the school internet.
- Only use websites which you are directed to. (Don't go on inappropriate websites!)
- I understand that the school may check my files and monitor the internet sites I visit at school.
- Only go on the internet when the teacher asks you.
- Always ask permission before taking a photo or video of another person.
- Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.
- Always ask permission before changing any settings on your iPad.
- Charge your iPad every night ready for learning the next day.
- Always use the charger it came with.
- Bring your iPad to school every day, as it is a vital learning tool.
- Make sure you only take videos and photos in an appropriate setting (e.g., not in a bathroom, bedroom etc.)
- School is silent! (Turn your volume off in school)
- Always remember to take your iPad home at night.
- Only ever touch your own iPad. Only touch other devices if you have permission.
- Personalise your own iPad, with a screen saver and wallpaper appropriate for school.
- Keep all documentation in a safe place at home.
- When you are not using your iPad put it away in a safe place.
- Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).
- Always send polite and responsible messages, messages will be monitored.
- I understand school will provide me with some key apps for my learning and I must not delete them. School also provides a more secure network for me to access the internet than other WIFI networks.
- The apps that are on my iPad are appropriate for my age and will not be offensive to others.
- Always ask an adult before downloading additional apps and make sure they are age appropriate.
- I understand social networking apps or websites are not permitted in school.
- Always ask permission if linking your iPad with your family Apple ID. (Parent or Carers may have details they don't want you to access).
- The content on my iPad (e.g., apps, photos, notes, internet history) will be appropriate and not cause offence.
- I understand that my iPad is covered under your own insurance plan and the school cannot be responsible for anydamage or loss.
- I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionality at schoolif teachers deem so.
- I understand my device will be linked to our school's mobile device management system and the school can view con- tent on the device as well as enforce restrictions.
- I am clear that school retains the right to restrict any content deemed unsuitable.
- I am aware that my device will need to be configured by school, which includes a full reset of the device.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn't written above, don't do it!
You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

Child Name:		Parent/ Carer Name:	
Signature:		Parent/Carer Signature	
Date:		Date:	

Pupils, parents, carers, staff and governors all want Normanby Primary to be a safe and happy place, so that you can learn and enjoy your time at school. All of our policies reflect this, and we all should use any item of equipment in a sensible, kind and thoughtful manner.

Normanby Primary School

Appendix 6

NORMANBY PRIMARY SCHOOL
Ironstone Academy Trust
Acceptable Internet Use Policy for Visitors

Remember that we use Information Communication Technology and the Internet for learning!

- ✓ Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children's education, staff professional development or the broader aims of the school.
- ✓ I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or unprofessional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with the Trust Policy.
- ✓ Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
- ✓ I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on social media.
- ✓ Access must only be made via the user's authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
- ✓ Do not download, use or upload any material which is unsuitable for use within the school, or which compromises the security of the school network.
- ✓ Do not reveal or share any personal information or photographs about any member of the school, adult or child.
- ✓ Ensure that children using the Internet are supervised at all times.
- ✓ When using web sites in the classroom, always assess the web page before displaying it to children.
- ✓ Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
- ✓ I will use the 'cloud space' provided to store information that does not identify any children's personal details.
- ✓ I will not plug in any personal USB storage devices as they could infect our network with malicious software.
- ✓ I will only use encrypted school issued devices to store information and all devices much be password protected.
- ✓ Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
- ✓ If unsuitable material is accessed inadvertently, the school's IT Leader should be informed directly. Individual user's Internet access will be monitored, including websites visited and e-mail use.
- ✓ If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
- ✓ The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.

I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated, and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.

Name: Date:

Signed:

Appendix 6a

NORMANBY PRIMARY SCHOOL
Ironstone Academy Trust
Acceptable Internet Use Policy for Staff

Remember that we use Information Communication Technology and the Internet for learning!

- ✓ Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children's education, staff professional development or the broader aims of the school.
- ✓ I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or un-professional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with the Trust Policy.
- ✓ Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
- ✓ I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on social media.
- ✓ Access must only be made via the user's authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
- ✓ Do not download, use or upload any material which is unsuitable for use within the school, or which compromises the security of the school network.
- ✓ Do not reveal or share any personal information or photographs about any member of the school, adult or child.
- ✓ Ensure that children using the Internet are supervised at all times.
- ✓ When using web sites in the classroom, always assess the web page before displaying it to children.
- ✓ Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
- ✓ I will use the 'cloud space' provided to store information that does not identify any children's personal details.
- ✓ I will not plug in any personal USB storage devices as they could infect our network with malicious software.
- ✓ I will only use encrypted school issued devices to store information and all devices much be password protected.
- ✓ Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
- ✓ If unsuitable material is accessed inadvertently, the school's IT Leader should be informed directly. Individual user's Internet access will be monitored, including websites visited and e-mail use.
- ✓ If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
- ✓ The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.

I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated, and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.

Name: Date:

Signed:

Appendix 6c

Normanby Primary School Digital Image Consent

Date and Event

Please sign below if you are intending to use a video camera, digital camera or any other recording device, including mobile phones to record images of the school performance on the date specified above.
Images can only be used on the understanding they are only viewed (used) in the home environment and not shared by digital or other means

Any photographs taken at school events are for personal use only and we ask that they are not published online including on social networking sites such as Facebook. As you are aware we seek permission for online publication and not all parents agree to photographs being published online for a number of reasons including serious child protection concerns. As a school it is important that we fully respect the privacy of such pupils, and we thank you for your support in this.

Child:	Name:	Signature:	Intended device:

Appendix 7
Committing Illegal Acts

Committing an Illegal Act - Did You Know?

1 Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

2 If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

3 Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

4 Showing anyone else illegal material that you have received **is an illegal act**

5 Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

6 Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material

7 **Within 4 simple steps you could easily break the law 4 times. Each is a serious offence**

8 Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

9 Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening.** Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

Appendix 8
NPS Bi-annual Consent form

Normanby Primary School Combined Bi-annual Consent Form

Images and videos parental consent form

This form explains the reasons why and how Normanby Primary School may use images and videos of your child. Please read the form thoroughly and outline your agreement as appropriate.

Why do we need your consent?
Normanby Primary School requests the consent of parents on a bi-annual basis to use images and videos of their child for a variety of different purposes.
Without your consent, the school will not use images and videos of your child. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why do we use images and videos of your child?
Normanby Primary School uses images and videos of pupils as part of school displays to celebrate school life and pupils' achievements; to promote the school on social media and on the school's website; and for other publicity purposes in printed publications, such as newspapers.
Where the school uses images of individual pupils, the name of the pupil will not be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil will not be used to accompany the text.
If, for example, a pupil has won an award and their parents would like their name to be published alongside their image, separate consent will be obtained prior to this.
Normanby Primary School may take images or videos of individual pupils and groups of pupils to use on social media, the school website, in school prospectuses and other printed publications, such as a newsletter.

Who else uses images and videos of your child?
It is common that the school is visited by local media and press, who take images or videos of school events, such as sports days. Pupils will appear in these images and videos, and these may be published in local or national newspapers, or on approved websites.
Parents, carers and other visitors may attend school for a range of reasons. If photography is allowed at these events, the school will keep a register of individuals who choose to do so. School will give advice that these images are for personal use, and that images of other children must not beshared on social media.
The following organisations may use images and videos of your children:

- Evening Gazette
- BBC, ITV and other Television and Media Channels

Where any organisations other than those above intend to use images or videos of your child, additional consent will be sought before any image or video is used.
What are the conditions of use?

- This consent form is valid for the current 2018/2019 academic year and for the following year.
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.

- The school will not use the personal details or full names of any pupil in an image or video, on our website, in our school prospectuses or any other printed publications.
- The school will not include personal emails or postal addresses, telephone or fax numbers on images or videos on our website, in our school prospectuses or any other printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school may use group or class images or videos with general labels, e.g., 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e., it would not be suitable to display an image of a pupil in swimwear.
- The school will take class images of your child which are available to purchase annually.

Parental consent form for receiving marketing material

This form explains the reasons why and how Normanby Primary School may send you marketing material. Please read the form thoroughly and outline your agreement as appropriate.

Why do we need your consent?

Normanby Primary School requests the consent of parents on a bi-annual basis to send them marketing material, e.g., flyers, from organisations associated with the school, such as the PTFA, Music Works, Tom Burke Academy, Simon Carson Sports School and Chris Nixon Music Services. Without your consent, the school will not send you any marketing material. Similarly, if there are only certain conditions under which you would like to receive marketing material, the school will abide by the conditions you outline in this form.

Why are we sending you marketing material?

Normanby Primary School uses marketing material to promote the events that are taking place at school, for example the summer fair. Events which raise money for the school are only successful if the school receives support from the parents of its pupils; therefore, we feel it is important to obtain your consent to send you promotional material.

You are under no obligation to respond to any marketing material, and we appreciate that it may not always be feasible for you to do so. Through sending marketing material, our primary aim is to inform you of the events that are taking place during the school year and, if you wish to take part in them, how you can do so and to what benefit.

What are the conditions of use?

- This consent form is valid for the current 2018/19 academic year and the following year
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not send any marketing material to parents that has not already been consented to.
- The school will not share this list with any third parties without prior consent from parents.
- The school will not send any marketing material to parents if it is not already mentioned in this form.

ICT acceptable use agreement for primary pupils

At Normanby Primary, pupils are expected to:

- Only use ICT on the school premises for studying purposes.
- Use the class or school e-mail address when sending or receiving emails.
- Only open email attachments from people known to them or people who the teachers have approved.
- 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 offensive language, pupils will report it to theirteacher.
- 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, its employees and pupils.
- Only store and use images of pupils for school or private purposes, acting in line with the school's IT Policy, 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 ca is not held responsible for children accessing inappropriate materials/ the nature of all the content hosted on the internet

Summary Code of Conduct and Home School Agreement

This Agreement should be read in conjunction with information on our website and does not replace our Policies

For children to achieve success at school it is important that parents, children and the school are able to work together, each party having an equally significant part to play in the partnership. In order that this partnership can work effectively, each party must be supportive of the other and committed to working in the best interest of all concerned.

Normanby Primary School will endeavour to: -

- Provide a caring, well-ordered and stimulating environment.
- Offer a broad and balanced curriculum to pupils of all abilities.
- Achieve high standards of work through encouraging all pupils to do their best at all times, feel proud of their achievements and enjoy being a valued member of the school.
- Encourage the children to behave appropriately at all times.
- Keep you informed about general school matters and about your child's progress, attitude and behaviour in particular.
- Be open and welcoming at all times and offer a variety of opportunities for you to become involved in the school community.

Parents will endeavour to:

- Ensure regular attendance, punctuality and appropriate dress.
- Notify the school if, for any reason, my child cannot attend.
- Help my child to take an interest in their work and sustain effort and achievement.
- Let the school know about any matters which may affect my child at school.
- Support and encourage my child with homework and other opportunities for home-learning.
- Encourage my child to follow the school's Rights and Responsibilities structure and Healthy School activities.

Parents and Carers should be aware that the school follows the system of Safeguarding and Child Protection detailed in 'Keeping Children Safe in Education' and by the Local Safeguarding Board. This governs how we relate to other agencies, and this sets up the framework for how staffare trained and subsequently deliver their responsibilities.

Refreshing your consent

This form is valid for the entire academic year, 2018/19 – it will be updated on a bi-annual basis. Parents are required to fill in a new form for their child alternate academic years.
Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g., an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g., safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g., amending the provisions for which consent has been provided for new requirements for consent, e.g., an additional form of distributing marketing material
- Changes to school circumstances, e.g., if a new headteacher reviews how the school markets itself
- Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Head of School. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Head of School. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent
Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing images or videos that were shared prior to withdrawal; however, the school will make a reasonable effort to remove images of the pupil where possible, e.g., images of the pupil on the school's website will be removed.
If you would like to withdraw your consent, you must submit your request in writing to the Head of School.

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 Normanby 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 my requirements.
- The reasons why Normanby 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 my consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the Head of School

Name of parent: _____

Signature: _____

Date: _____

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

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 use images of my child to publicise school events and activities (only including the organisations outlined above).		
The local media use videos of my child to publicise school events and activities (only including the organisations 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. This includes 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 PTFA, The governing board, The Leadership Team		
Receiving marketing material from the third-party organisations, judged appropriate by the Head of School		
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.		