E-SAFETY POLICY

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to e-safety, including:

- The policies and practice embedded in our school and followed by the who school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to e-safety incidents
- A progressive, age appropriate e-safety curriculum for all pupils

E-safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

- The development of our safety policy involved:
  - o The Headteacher
  - o The Designated Person for Child Protection
  - o The Computing Subject Leader
  - o Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

     o The governor responsible for Safeguarding

It was presented to the Full Governing Body on and ratified on 28th November 2016 and will be formally reviewed in November 2017.

- This policy may also be partly reviewed and / or adapted in response to specific e-safety incidents or developments in the school's use of technology. It has been shared with all staff at a staff meeting and is readily available on the school network and website.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As E-safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Person for Child Protection and governors.

RATIONALE

At Orchard Park, we believe that the use of technology in schools brings great benefits to both teachers and pupils. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology safely and effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.
Technologies regularly used by pupils and staff include:

Staff:
- Staff laptops and also desktops in the office and library, including staff level internet access, server access and access to MIS systems.
- Some staff have access to MIS systems from home via a secure logon and keyfob. Staff laptops can also be used at home in accordance with the staff AUP.
- Curriculum and staff iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and interactive whiteboards.

Pupils:
- Curriculum iPads and desktops in the library and some classrooms including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, control equipment, class cameras etc).

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

THE E-SAFETY CURRICULUM

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate e-safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- **At KS1:** 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.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Orchard Park we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.
This is achieved using a combination of:
- Discrete and embedded activities drawn from a selection of appropriate materials including the ACE (Accredited Competence in E-safety) scheme of work.
- Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.
- Key e-safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.
- SMART rules are displayed in all areas were children access online resources. Laptops and computers have SMART rules as wallpaper, as a constant reminder of online safety (see Appendix One).

CONTINUED PROFESSIONAL DEVELOPMENT

- Staff at Orchard Park receive up-to-date information and training on e-Safety issues in the form of staff meetings and updates from Computing Subject Leader, as well as training from external providers where appropriate.

- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

SCHOOL WEBSITE

Schools are required to publish certain information online. The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.
In conjunction with a range of online services, a school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Head teachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

MONITORING, AND AVERTING E-SAFETY INCIDENTS

The school keeps children safe when using online technologies through a combination of e-safety education, filtering and monitoring children's online activity and reporting incidents, including following Child protection procedures where appropriate.
The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network. Managed firewalling.

- Base line and enhanced filtering provided by the LA supported approved filtering system

- CPSN provided Sophos antivirus package

- Council funded email system for all school staff with direct internal routes to the council for trusted email communications.

- Restrictions on download of software, apps and file types from known compromised sites

Staff also monitor pupils' use of technology and, specifically, the internet.

- Pupils' use of online services (including the World Wide Web) are supervised in school at all times allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network.
- Visitors to the school can access part of the network using a generic visitor login and password
- The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.

The school recognises its duty to educate and inform the parent body of potential online dangers. As a result, the school will host e –safety events and share latest e safety concerns in the school newsletter.   This will include links to parenting websites that will provide additional online information and advice.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

RESPONDING TO E-SAFETY INCIDENTS

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to e-safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an e-safety incident occurs, Orchard Park Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern with parents (where appropriate) before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

APPENDIX 1 – ONLINE SMART RULES

Be smart on the internet

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

m MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

a ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

r RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

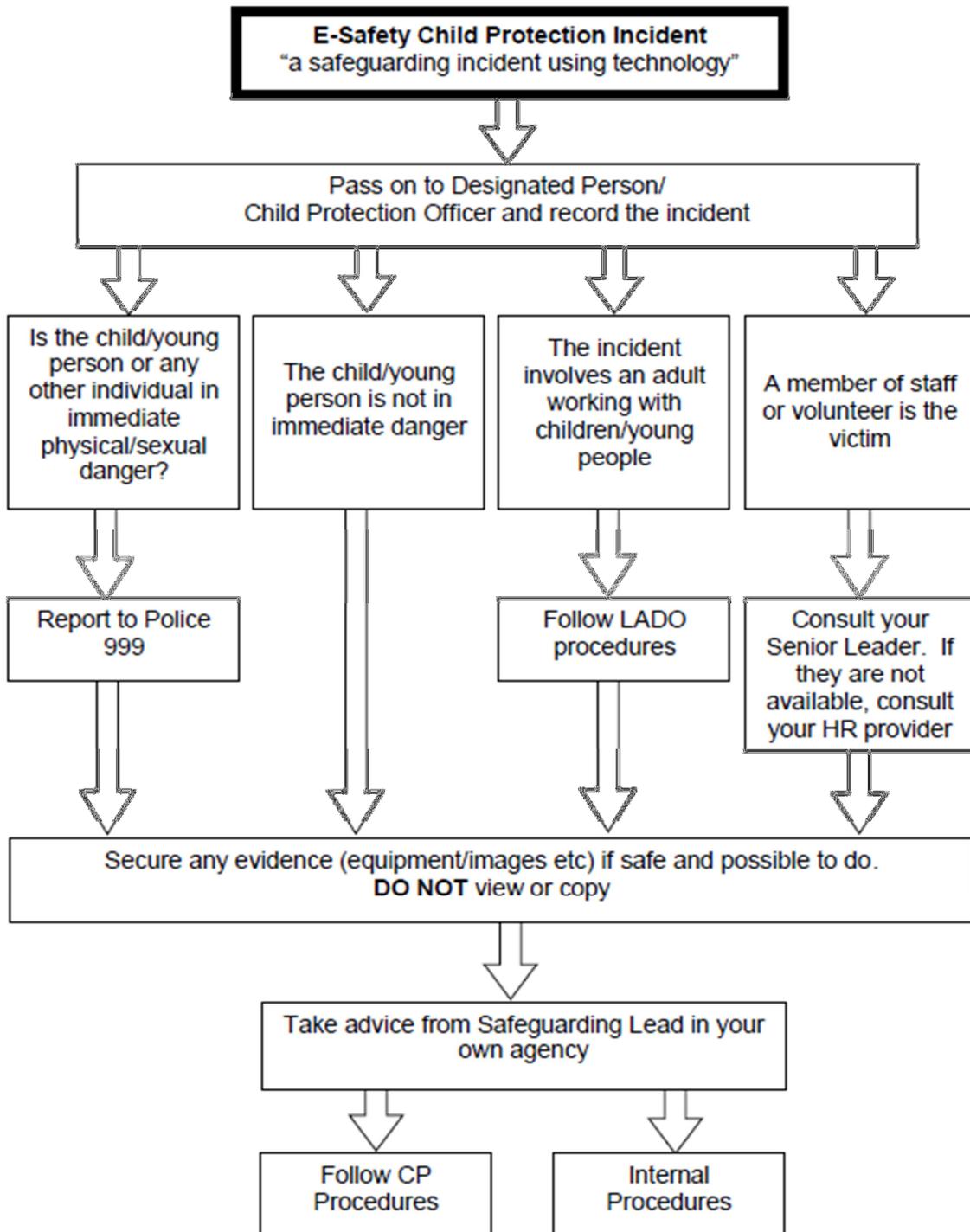You can report online abuse to the police at www.thinkuknow.co.uk

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

APPENDIX 2

You come across a child protection concern involving technology ...

E-Safety Child Protection Incident
"a safeguarding incident using technology"

↓

Pass on to Designated Person/
Child Protection Officer and record the incident

↓

Is the child/young person or any other individual in immediate physical/sexual danger?	The child/young person is not in immediate danger	The incident involves an adult working with children/young people	A member of staff or volunteer is the victim
↓		↓	↓
Report to Police 999		Follow LADO procedures	Consult your Senior Leader. If they are not available, consult your HR provider

↓

Secure any evidence (equipment/images etc) if safe and possible to do.
DO NOT view or copy

↓

Take advice from Safeguarding Lead in your own agency

↓

Follow CP Procedures	Internal Procedures

<u>APPENDIX 3 - STAFF E-SAFETY ACCEPTABLE USE POLICY</u>

<u>USE OF SCHOOL BASED EQUIPMENT</u>

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the computing (and e - safety) co - coordinator/ headteacher/ prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the computing and e-safety coordinator/ Headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the office manager/ computing/e-safety coordinator.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the network manager/ SIRO.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

SOCIAL NETWORKING

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the Headteacher.

MANAGING DIGITAL CONTENT

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy/ Home School Agreement (or any other relevant policy).
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

EMAIL

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect myself. As and when I feel it necessary,

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

> I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.

- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

MOBILE PHONES AND DEVICES

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

LEARNING AND TEACHING

- In line with every child's legal entitlement I will ensure I teach age an appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

STAFF iPADS

This AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

Users in breach of this responsible use policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

- The iPad has been provided by the school for professional use by staff and should not be used by anyone other than the member of staff, including family members.
- All staff must set a passcode on their iPad to prevent others from misusing it.
- ITunes account passwords should not be shared with anyone else.
- Passwords should not be shared -misuse of passwords, codes or other unauthorised access is not acceptable.
- Individual members of staff are accountable for any activity on their mobile device.
- Downloaded apps must be for educational use only e.g. using in school or testing for school.
- Use of websites etc. should echo the school's approach to acceptable use of laptops.
- Images of pupils should be transferred off the device to the school server before the iPad is taken off site.
- Personal images should not be stored on school ipads
- To prevent access to confidential information, staff iPads should not be used by pupils (at school's discretion).
- Accessing inappropriate material – all material on the iPad must adhere to the school ICT Responsible Use Policy. Ie users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Illegal activities – use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity is not allowed.
- Cameras – users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Leadership team.
- Individual users are responsible for the setting up and use of any home internet connection and no support will be provided for this by the school.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

<u>RESPONSIBLE USE of iPADS BY EVERYONE</u>

- Protective covers/cases must be used at all times.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused- care should be taken to handle and hold the iPad safely and securely and avoid placing heavy objects (books, laptops, etc.) on top of the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Store out of sight (preferably in the boot) in vehicles.
- Users should not photograph any other person, without that person's consent. Images of other people may only be made with the permission of those in the photograph.
- The iPad is subject to routine monitoring. Devices must be surrendered immediately upon request by any senior member of staff.
- Staff must take responsibility for all personal files that may be deleted from an iPads.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.

AGREEMENT

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :	
Role in School:	
Signed	
Date:	
Accepted by:	
Date:	

Our Mission Statement

A place where children are empowered to reach their full potential, with the highest possible aspirations and passion for learning. With values and respect, our children are confident to move from our nurturing environment to explore and succeed in the wider world.