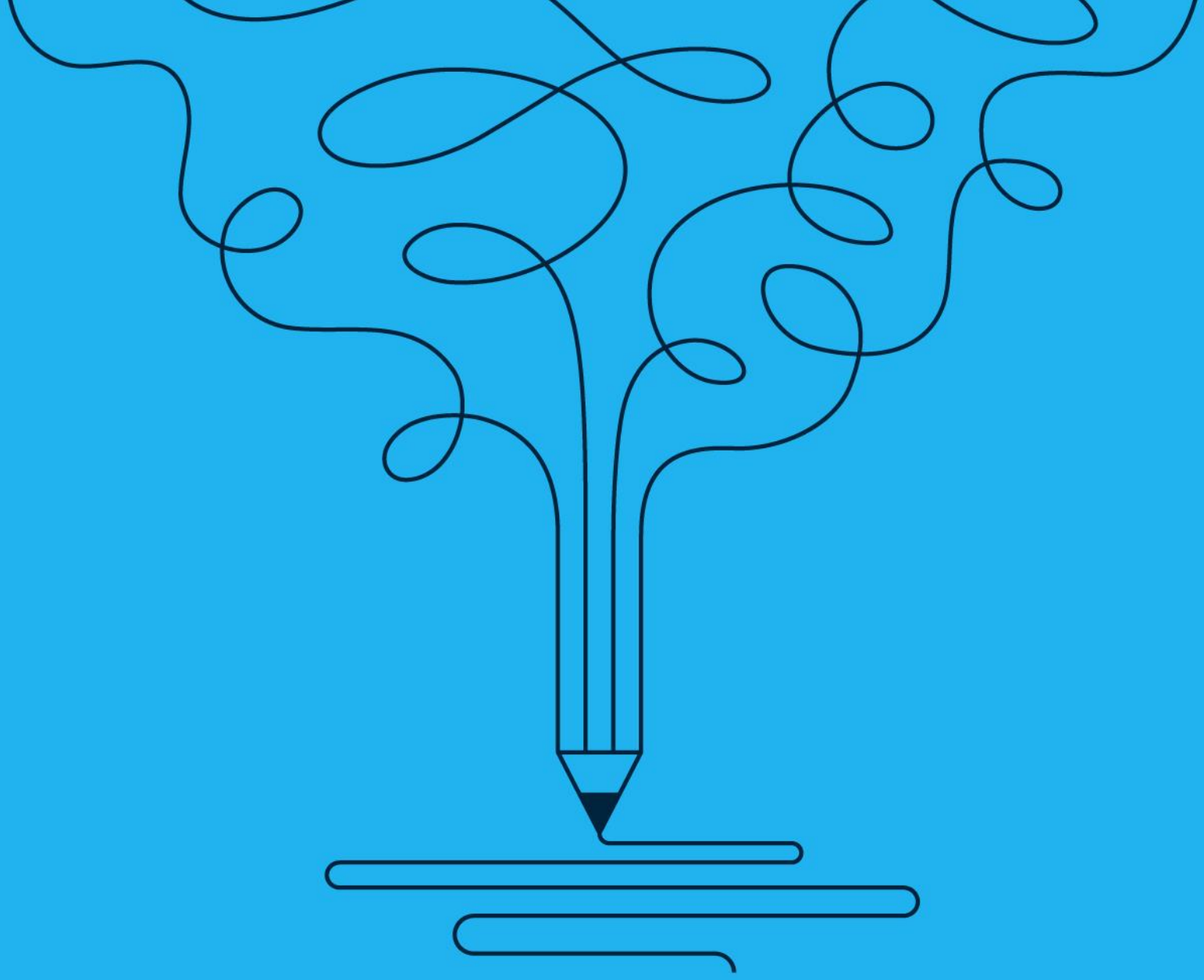

ACCEPTABLE USE AND E-SAFETY POLICY

AUTHOR	REVIEWED	NEXT REVIEW
R. HORTON	SEPTEMBER 2017	SEPTEMBER 2019

OULTON
PRIMARY SCHOOL

1 Introduction

The purpose of this document is to ensure that all users (staff, governors, secondments, visitors etc.) of Oulton Primary School's computing facilities are aware of Oulton's policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of Oulton Primary School. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes the School to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.

It is the responsibility of all users of Oulton Primary School computing facilities to be aware of and follow all of the School ICT policies and guidelines and to seek advice in case of doubt. Oulton Primary School's Computing policies are published under the School Policies section on Staffworks Drive. A copy of this policy is also available on the school website.

This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes. This policy should be used in conjunction with the school's Child Protection Policy, Anti-Bullying Policy, Computing Policy and Staff Disciplinary Policy.

Oulton Primary School encourages the use of school computing facilities for the mutual benefit of its staff and pupils. Similarly, the regulations that constitute this policy seek to provide for the mutual protection of Oulton Primary School and the rights of its staff and pupils.

2. E-Safety policy

The E-Safety Policy relates to other policies including those for Computing, Bullying and for Child Protection. The school will appoint an E-Safety Leader. Ideally, the E-Safety Leader is also a Designated Child Protection Teacher as the roles overlap; this is the current situation.

The Designated Person for E-Safety is: Richard Horton, who is also a Designated Teacher for Child Protection.

Our E-Safety Policy has been written by the school, building on the Leeds E-Safety Policy and government guidance. It has been agreed by senior management and

approved by governors. The E-Safety Policy and its implementation will be reviewed annually. The E-Safety Leader will attend regular training (no longer than every two years) and this training will be fed back appropriately to all members of the school community to ensure that it is embedded in the ethos of the school.

The E-Safety and Acceptable Use Policy was created by: Richard Horton Deputy Head Teacher/ Computing Leader

Date of Review: September 2017

Date of next review: September 2019

It was approved by the Governors on:

2.1 Roles and Responsibilities

The Management Team (SLT) accepts the following responsibilities:

- Identify a person (the E-Safety Leader) to take responsibility for E-Safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-Safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of the E-Safety Leader

- Promote an awareness and commitment to E-Safety throughout the school
- Be the first point of contact in school on all E-Safety matters
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy

- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on E-Safety issues to the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance
- Read, understand and adhere to the staff Acceptable Use Policy
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that personal social network pages are secured from general view and that content does not bring the school or themselves into disrepute
- Do not mention the name of the school on social networking sites including as part of their profile
- Take ultimate responsibility for the content and comments on their personal Social Media sites and pages
- Embed E-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable

- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Additional Responsibilities of Technical Staff (School ICT Services)

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any E-Safety related issues that come to their attention to the E-Safety Leader and/or Leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the School ICT equipment
- Liaise with the Local Authority and others on E-Safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil Acceptable Use Policy and follow all safe practice guidance
- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the pupil Acceptable Use Policy with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

2.2 Teaching and learning

Why Internet use is important

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

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly (Usually daily- automatically over the school network)

E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.

Pupil's work can only be published with the permission of the parents.

Social networking and personal publishing

The school will block/filter access to social networking sites. These will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Photographs, Videos, and Indecent images

Below are the specific expectations for the use of photographic materials from the document "Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings" DSCF 2009

Working with pupils may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of pupils. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.	**This means that adults should:** □ be clear about the purpose of the activity and about what will happen to the images when the activity is concluded □ be able to justify images of children in their possession □ avoid making images in one to one situations or which show a single child with no surrounding context

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them. Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. It is not appropriate for adults to take photographs of children for their personal use. **It is recommended that when using a photograph the following guidance should be followed:** □ if the photograph is used, avoid naming the pupil □ if the pupil is named, avoid using their photograph	□ ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed. □ only use equipment provided or authorised by the school □ report any concerns about any inappropriate or intrusive photographs found □ always ensure they have parental permission to take and/or display photographs **This means that adults should not:** □ display or distribute images of children unless they have consent to do so from parents/carers □ use images which may cause distress □ use mobile telephones or any other similar devices to take images of children □ take images 'in secret', or taking images in situations that may be construed as being secretive.

□ schools should establish whether the image will be retained for further use □ Images should be securely stored and used only by those authorised to do so.	
There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to their school/service to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. Adults should ensure that pupils are not exposed to any inappropriate images or web links. School/service and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g.	**This means that schools/services should** □ have clear E-Safety policies in place about access to and use of the internet □ make guidance available to both adults and pupils about appropriate usage. **This means that adults should:** □ follow their school/service's guidance on the use of IT equipment □ ensure that children are not exposed to unsuitable material on the internet □ ensure that any films or material shown to pupils are age appropriate

personal passwords should be kept confidential. Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.	

Managing filtering

The school will continuously monitor the effectiveness of its filtering systems and improve as necessary.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader who will ask School ICT to block future access to the site. The E-Safety Log should then be completed.

Managing videoconferencing

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

Videoconferencing is only to take place as part of pre-arrange and risk assessed activities.

Managing emerging technologies

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

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

No photographs or videos of school activities and/or pupils are to be taken and/or stored on personal mobile phones or computers.

All photos are to be stored centrally on the school network (S:\\). No photos/videos should be stored on school equipment that leaves the premises (School laptops, tablets, ipads, etc.)

Staff will be issued with a school phone where contact with pupils/parents is required e.g. school residential visits/trips.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

Authorising Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access where reasonable steps/systems by the school have been put in place to prevent such access.

The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures.

Pupils and parents will be informed of the complaints procedure.

Where necessary, discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to E-Safety. This may involve parental information sessions and where possible, advice about E-Safety matters at home.

2.5 Communications Policy

Introducing the E-Safety policy to pupils

E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored. The new Computing Scheme of Work (2016) has specific E-Safety content that must be delivered to each year group.

Staff and the E-Safety policy

All staff will be given access to the School E-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure, parental workshops and on the school Web site.

2.6 Protecting Individual User Profiles

It is the responsibility of all users issued with a computer username and password to keep these details secret. It is essential that strong passwords are used (containing at least a capital and a numeral). Passwords must be changed regularly, identical passwords must be used on laptops and the school network (to ensure continued access to network and printing resources). Occasionally, School ICT may implement a forced password change across the site.

Teaching staff with laptops should ensure that they enable a screensaver on a short delay (5 minutes) that requires staff to re-enter their passwords before regaining access to the system. Laptops should also be set up so that closing the lid makes the computer 'sleep' this option also requires a password when is restarted. Where laptops are to be used for displaying content on a Smart Board, the screensaver can be temporarily disabled and enabled again once finished.

Staff must ensure that their laptop/workstation is locked before leaving it unattended. This is especially important due to the access to sensitive data, pupil data, personal data and SIMS data that could be achieved by leaving a computer unsecured. Users are required to ensure that personal/sensitive data is kept securely as per the provisions of the Data Protection Act 1998.

The youngest members of the school (FS/KS1) will be issued with generic passwords that are easy for them to use and remember. As pupils move into KS2, pupils are required to use a personalised and unique password. A secure copy of these passwords will be kept by School ICT to aid the resetting of forgotten passwords. Pupils must keep their passwords secret; this is reinforced during E-Safety lessons.

2.7 Cyber-Bullying

In line with the school's anti bullying policy, the school will not tolerate bullying and will act swiftly to resolve any incidents of Cyber-Bullying. Further details can be found in the school's Anti-Bullying policy.

What Is Cyber-Bullying?

"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."[1]

Cyber-bullying is the use of ICT, commonly a mobile phone or the internet, deliberately to upset someone else. It can be used to carry out all the different types of bullying; an extension of face-to-face bullying. It can also go further in that it can invade home/personal space and can involve a greater number of people. It can take

[1] Research commissioned by the Anti-Bullying Alliance from Goldsmiths College, University of London

place across age groups and school staff and other adults can be targeted. It includes: threats and intimidation; harassment or ‘cyber-stalking’; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images and manipulation.

Seven categories of cyber-bullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

What can schools do about it?

While other forms of bullying remain prevalent, cyber-bullying is already a significant issue for many young people. Oulton Primary recognises that staff, parents and

young people need to work together to prevent this and to tackle it whenever it occurs.

School Governors, the Head teacher and entire school have a duty to ensure that: bullying via mobile phone or the Internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with cyber-bullying in school[2].

We ensure that:

- The curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely including personal rights
- All e-communications used on the school site or as part of school activities off-site are monitored
- Clear policies are set about the use of mobile phones at school and at other times when young people are under the school's authority
- Internet blocking technologies are continually updated and harmful sites blocked
- They work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice
- Security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside school
- They work with police and other partners on managing cyber-bullying.

ICT and Mobile Phone Policy

If a cyber-bullying incident directed at a child occurs using e-mail or mobile phone technology, either inside or outside school time, we will take the following steps:

- Advise the child not to respond to the message
- Refer to relevant policies, e.g. E-Safety and Acceptable use, Anti-Bullying and PSHE and apply appropriate sanctions

[2] The School Standards and Framework Act 1998 require schools to have anti bullying policies; the anti-bullying policy should include or refer to a cyberbullying policy. The ICT policy should also refer to cyberbullying

- Secure and preserve any evidence
- Inform the sender's e-mail service provider
- Notify parents of the children involved
- Consider delivering a parent workshop for the school community
- Consider informing the police depending on the severity or repetitious nature of the offence. The school recognises that some cyber-bullying activities could be a criminal offence under a range of different laws including: *The Protection from Harassment Act 1997; the Malicious Communication Act 1988; section 127 of the Communications Act 2003 and the Public Order Act 1986*

If malicious or threatening comments are posted on an Internet site or Social Networking Site about a pupil or member of staff, we will also:

- Inform and request that the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to www.ceop.gov.uk/contact_us.html if of a sexual nature
- Endeavour to trace the origin and inform the police as appropriate.

Working with Parents

Oulton Primary School has developed a home-school agreement that includes clear statements about e-communications. The school seeks to regularly update parents on:

- What to do if problems arise
- E-communication standards and practices in school
- What's being taught in the curriculum
- Supporting parents and pupils if cyber-bullying occurs by:
    - ✓ Assessing the harm done
    - ✓ Identifying those involved
    - ✓ Taking steps to repair harm and to prevent recurrence

Preventing Cyber-Bulling

All staff will be helped to keep up to date with the technologies that children are using.

- Pupils will be educated about cyber-bullying through a variety of means: assemblies, conferences, Anti-bullying Week.
- Pupils will sign an Acceptable Use Policy. (see Appendix)
- Parents will be provided with information and advice on cyber-bullying via literature, meetings, etc.

- Pupils, staff and parents will be involved in evaluating and improving policies and procedures.

Reporting Cyber-Bulling

The Head teacher, E-Safety Leader, designated members of staff for Child Protection, and designated Governor for Child Protection will:

- Ensure staff can recognise non-verbal signs and indications of cyber-bullying.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
- Publicise to all members of the school community the ways in which cyber-bullying can be reported.

Sexting

'Sexting' is the sending of inappropriate pictures via mobiles and other devices. The images sent might be of the person sending it or it might be an image that they are passing on. All indecent pictures of children under 18 are classed as child abuse pictures and are illegal, even if it is in the possession of the person in the photo. If any staff become aware of such content on a device, they must follow the procedure below:

1. Consult SLT and Designated Child Protection Teachers
2. Confiscate the device and store securely
3. SLT/Designated teachers to investigate and conduct a risk assessment
4. Ensure appropriate support is given to the young person
5. SLT/Designated teachers to consult and inform parents

6. SLT/Designated teachers to consult Children's Services and make a referral if necessary

As set out in the DFE guide 'Screening, searching and confiscation'

https://www.gov.uk/government/publications/searching-screening-and-confiscation

If staff believe that there is content on a pupil's phone/electronic equipment that is pornographic or and E-Safety issue, it is lawful for staff to confiscate the device to preserve any evidence. This power is advocated by the Child Exploitation and Online Protection Centre (CEOP) as part of their training programme to ensure that E-Safety issues are dealt with appropriately.

2.8 Staff use of Social Media/Networks outside of the school day

Many members of staff use Facebook and other social media sites. Due to the nature of our profession, it is especially important that we keep our personal and professional lives separate online. Care must be taken to ensure that you do no bring yourself or the school into disrepute. Following these steps can help to make sure that your personal use of social media does not impact on you professionally. However, this list not exhaustive and staff should use a common sense approach when working online: think before you post… would you say this to the Head Teacher? Failure to follow the steps below and/or using social networks recklessly may result in disciplinary action being brought against you. YOU are ultimately responsible for the content on your own personal Social Media Site; great care should be taken to stop unauthorised access to your account.

- Ensure that you set your security settings appropriately- make sure that your profile is not viewable to people who are not your friends.
- Be choosey about which friend requests you accept. Support to customise your settings can be provided by us if needed.
- Your social media page should not contain any references to school including listing the school as your work place.
- Discussions about school should not take place on social networks with staff or other members of the public. For the purposes of discussions about school, staff should use their work email account to conduct discussions with colleagues. All other communication about the school to all other parties

should take place via the official school channels with the approval of a member of the SLT.

- Ideally, school staff should not be Facebook friends with parents of children in the school. This may be a contentious point, as many staff are parents of children in the school. If you have got parents as Facebook friends, consider whether you need that online friendship. If it is necessary, try and limit the content that they can see on your page by changing their individual permissions or adding them to the 'Limited Profile' group.
- Under no circumstances should staff add pupils from our school to social media sites. It is also not desirable for staff to be friends with ex-pupils where there are no reasonable grounds for such friendships. The term 'reasonable' will be decided upon by the school on a case by case basis.
- Be selective about what photos are uploaded onto social media sites- photos of boozy staff nights out are discouraged. If photos are uploaded of staff, ensure that they are not 'tagged' or posted onto any account which parents can view (an unprotected account or an account with friends who are parents).
- Do not leave your Social Media account logged in, allowing misuse by others. You are ultimately responsible for the content on your personal page and proving that something was posted by a third party is especially difficult.
- Location tagging- be mindful of tagging yourself and colleagues in particular locations during and out of school hours. Again, this information may be easily viewable by other members of the school community. Location tagging **should not** be used by staff whilst on school visits. This is a serious safeguarding issue as it potentially allows people who are not allowed contact with certain children to know exactly where they are, in a place that is often not as secure or as well-staffed as school.
- Please ensure that you do not post anything about the school on your profile. Communication with parents should be conducted via certain routes only (school phone, school mobile, school email and school's official Twitter feed). Whilst on a trip, it is the responsibility of the visit leader or deputy to communicate with parents, via the school as necessary.

2.9 Acceptance of the E-Safety policy

All users of the schools computing hardware, software and systems (as detailed below) must accept the terms of the above sections. By signing the E-Safety agreement, all pupils, staff, governors, visitors and supply staff agree to uphold the provisions of this policy. Non-compliance may result in loss of access to the school system, referral to staff disciplinary procedures and in the case of a serious breach, to the police or other official bodies.

Copies of the different E-Safety agreements can be seen as an appendix.

3. Computing facilities

Access to school computing facilities is managed by an appointed ICT Network Manager. Use of any of Oulton Primary School's computing facilities is at the discretion of Oulton Primary School.

3.1 Definition

The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Oulton Primary School and any allocation of time, memory, disk space or other measure of space on any of Oulton Primary School's hardware, software or networks

3.2 Ownership

Computing facilities owned by Oulton Primary School and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Oulton Primary School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

3.3 Desktop PCs

Desktop PCs are a critical asset to Oulton Primary School and must be managed carefully to maintain security, data integrity and efficiency. Users must consult School ICT before installing non-standard software on computers managed by School ICT as a Desktop PC. Non-standard software shall be interpreted as any

software that does not comply with the regulation of the ‘Software’ sub-section below.
All users have access to appropriate areas on Oulton Primary School’s file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity.

Desktop PCs include the CPU/hard-drive unit and monitor both of which are subject to change.

3.4 Laptop PCs

Laptop PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of Oulton Primary School systems and data procedures, passwords or authentication devices for gaining remote access to Oulton Primary School systems must not be stored with the computer. This includes the saving of passwords into remote access software.
Highly confidential data can be encrypted to protect it in the event of Laptop PC loss. School ICT can help with this process.

If your Laptop PC is lost or stolen School ICT must be notified as soon as possible and a report made to the police.

3.5 Handheld and Mobile Devices

Handhelds and mobiles, including ipads/ipod touch, are at high risk from theft due to their size and nature of usage. Loss of the device can expose Oulton Primary School to a large liability through fraudulent use. It is therefore vital that staff are vigilant in caring for their security.
Oulton Primary School should take care to keep these devices concealed when not in use and to be conscious of onlookers who may be targeting devices for theft. In the event that a device is stolen, Oulton Primary School will be expected to report the theft to the police, obtain an incident number and contact School ICT as soon as possible

3.6 Loan Equipment

Policy regarding loan equipment is similar to that for laptops and handheld or mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.
If loan equipment is stolen or lost, School ICT should be informed immediately. It may also be that the user responsible for its care has to report the theft to the police and report the incident number to School ICT.

Any member of staff wishing to borrow equipment should seek permission from the head teacher or School ICT beforehand and must complete details in the loan register, kept in the Office.

3.7 Software

Only software properly purchased and/or approved by the Computing Manager may be used on school hardware. Non-standard or unauthorised software can cause problems with the stability of school computing hardware and it is necessary to contact School ICT before the installation of such software. Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CDROM) when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence through School ICT. School ICT must be notified when such additional/new software is installed. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.
Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact School ICT who will be happy to assist in resolving any issues.

3.8 Data Security

You must only access information held on Oulton Primary School's computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or

other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.
It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up.

3.9 Personal Data and the Data Protection Act

Oulton Primary School maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the Agency's holding and processing of personal data.
It is the responsibility of all Oulton Primary School staff to ensure that personal data is held and processed within the terms of Oulton Primary School's notification and in compliance with the data protection principles.

Personal data shall be:

- obtained processed fairly and lawfully
- held for specified lawful purpose(s)
- not used or disclosed in a way incompatible with the purpose(s)
- adequate, relevant and not excessive for the purpose(s)
- accurate and up to date
- not kept longer than necessary
- available to the data subject
- Kept secure.

Oulton Primary School should note that all data and correspondence, including e-mail messages, held by Oulton Primary School may be provided to a data subject, internal or external, in the event of a subject access request.

3.10 Freedom of Information Act

Oulton Primary School is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. Employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held,

whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request under the Act.

3.11 Virus Protection

Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Remote users are responsible for maintaining up to date virus definitions on their computers and can contact School ICT for help as required.
Users must not intentionally access or transmit computer viruses or similar software.

Non-Oulton Primary School software or data files intended to be run on school equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer, stop using the computer, pull out the Network Cable/Turn off your Wi-Fi and contact School ICT immediately.

3.12 Network Access

Passwords protect Oulton Primary School systems from access by unauthorised people: they protect your work and the school's information. Therefore never give your network password to anyone else without your departmental manager's permission. Procedures are in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be re-used immediately.
Passwords must be eight or more characters long and include at least one numeric or non-alphabetic special character.

Oulton Primary School does not allow the connection of non-school computer equipment to the network without prior request and technical approval. This includes connection via dialup, Ad-hoc or Virtual Private Networking (VPN).

3.13 Further General Guidance

Oulton Primary School users must ensure prior approval at Head teacher level to:
Set-up World Wide Web sites on Oulton Primary School computing facilities

Publish pages on external World Wide Web sites containing information relating to Oulton Primary School

Enter into agreements on behalf of themselves or Oulton Primary School via a network or electronic system

Be used for external business interests or personal gain

4. Electronic mail

4.1 Use and Responsibility

Oulton Primary School's electronic mail (e-mail) system is provided for the school's purposes. E-mail is now a critical business tool but inappropriate use can expose Oulton Primary School and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements. The e-mail system costs the organisation time and money and it must be used judiciously in the same manner as other organisational resources such as telephones and photocopying.

School-wide e-mail messages must be business related and of significant importance to all staff.

4.2 Content

E-mail messages must be treated like any other formal written communication.
E-mail messages cannot be considered to be private, secure or temporary.
Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.
Improper statements in e-mail can give rise to personal liability and liability for Oulton Primary School and can constitute a serious disciplinary matter. E-mails that embarrass, misrepresent or convey an unjust or unfavourable impression of Oulton Primary School or its affairs, employees, suppliers, pupils are not permitted. Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable. Never send

confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.
Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 Privacy

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals e-mail, Oulton Primary School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee wrongdoing, protect the rights or property of the school, and protect ICT system security or to comply with legal process.
Messages sent or received may be copied and disclosed by Oulton Primary School for lawful purposes without prior notice.

It is not permissible to access or to send e-mail from another employee's personal account either directly or indirectly, unless you obtain that person's prior written approval.

5. Internet usage

The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.
Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Oulton Primary School Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable to expect Oulton Primary School employees to have good awareness and to be able to exercise good judgement. If in doubt over a specific case, please refer to the Head teacher or School ICT.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

All Internet usage from the Oulton Primary School network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant employees user account. Such an investigation may result in action via Oulton Primary School's Disciplinary Procedure and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

5.1 Newsgroups

Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing email as above.
Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Oulton Primary School. For example:

"The views expressed are my own and do not necessarily represent the views or policy of my employer."

5.2 Instant Messaging

Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, Oulton Primary School does not currently allow the use of instant messaging for the communication of sensitive or proprietary Agency information.

6. Private use, legislation and disciplinary procedures

6.1 Private Use

Computing facilities are provided for Oulton Primary School's school purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Oulton Primary School. Oulton Primary School does not accept liability for any personal loss or damage incurred through using the school computing facilities for private use.

6.2 Updates to this Policy

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all Oulton Primary School will be made when updates are available.

6.3 Relevant Legislation

The following are a list of Acts that apply to the use of Oulton Primary School computing facilities:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978

- Criminal Justice Act 1988
- Data Protection Act 1998
- General Data Protection Regulations 2018
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

6.5 Disciplinary and Related Action

Oulton Primary School wishes to promote the highest standards in relation to good practice and security in the use of information technology. All pupils, staff, governors, visitors and supply staff agree to uphold the provisions of this policy. Non-compliance may result in loss of access to the school system, referral to staff disciplinary procedures. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix A:

Examples of Behaviours Which Require the Use of the Oulton Primary School Disciplinary Policy

GROSS MISCONDUCT Examples

Criminal Acts – for example in relation to child pornography

Visiting pornographic sites (adult top shelf materials) except where this forms an authorised part of the employee's job (for example 'testing').

Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.

Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute

Downloading and installation of unlicensed products

Viewing sexually explicit materials, except where this forms an authorised part of the employee's job

Chat rooms – sexual discourse, arrangements for sexual activity

MISCONDUCT Examples

Frivolous use of Company computing facilities that risk bringing Oulton Primary School into disrepute.

Entering into contracts via the Internet that misrepresents Oulton Primary School. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Oulton Primary School is liable for this contract, without first consulting Oulton Primary School's financial procedures.

Deliberate Introduction of viruses to systems

This list is not exhaustive, but sets the framework of Oulton Primary School's approach to misuse of computing systems.

Oulton Primary School has the right to monitor employees' use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

Appendix B: Acceptable Use Policy for School Staff

I confirm that I have read and understood the **School's Acceptable Use and E-Safety Policy** and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

- Any content I post online (including outside school time) or send in an email from my school address will be professional and responsible and maintain the reputation of the school. I will not use social media to comment or talk about the school, staff, pupils or any other party.

- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.

- If I use instant messaging, chat rooms, webcams or forums for communicating with pupils or parents it will only be via a method agreed by the Head Teacher or Deputy Head Teacher.

- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager

- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils

- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school

- I will take all reasonable steps to ensure that all personal computers, laptops and memory devices are fully virus protected and that protection is kept up to date to reduce the risk of the school network becoming infected.

- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

- Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended- This is especially important when SIMS is logged in.

- I understand that I have the same obligation to protect school data when working on a computer outside school

- I will report immediately any accidental loss of confidential information so that appropriate action can be taken

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School's disciplinary procedures. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Name.....

Position……..

Signed.....

Date……

Appendix C: Acceptable Use Policy for temporary or supply staff and visitors to school

As a visitor to the school I recognise that it is my responsibility to follow school E-Safety procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school
- I will not use a personal computer I have brought into school for any activity which might be in conflict with my presence in the school
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned
- I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to contact pupils unless specific permission is given
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager

- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded
- If I have access to any confidential school information, pupil information or data it will only remove from the school site with permission and if so, it will be carried on a device which is encrypted or protected with a strong password
- I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the disciplinary procedures.

Name.....

Signed.....

Date……

Appendix D: Acceptable Use Policy for Primary Pupils in school.

- I will only use the school ICT equipment for purposes I have agreed with a member of staff
- I will keep my password and login private
- I will not interfere with anyone else's passwords, logins settings or files on the computer
- I will always seek permission before downloading material from the internet or using material I have brought into school because I understand the risks from virus infections
- I understand that I should only publish material on the internet that is my own work
- I know I need permission to take someone's photograph or video them
- Any messages I post on the Learning Platform or send in an email will be polite and responsible
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I will inform an adult if I see or receive any unpleasant material or messages
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I understand that the school may check my use of ICT and contact my parent/carer if they are concerned about my E-Safety
- I understand that the school may talk to my parent or carer if they are worried about my E-Safety

- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside school.

Pupil name.....

Signed.....

Appendix E: Acceptable Use Policy for community users of school computers

As a user of the school's computers I recognise that it is my responsibility to follow school procedures for the safe use of computers and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all means of electronic communication equipment belonging to the school and any personal devices which I bring into school in a responsible manner and in accordance with the following guidelines:

- I will only use the school computers for purposes related to the work I am completing in the school
- I will not use a personal computer I have brought into school for any activity which might be in conflict with my presence in the school
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school and the pupils
- I will not give any personal contact details such as email address, mobile phone number, IM account details to any pupil in the school. I will not arrange to VC or use a web camera with pupils unless specific permission is given by the school
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices are fully virus protected and that protection is kept up to date
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules my use of school facilities may be withdrawn.

Name.....

Signed.....

Date…….