MOWDEN HALL SCHOOL
E-SAFETY POLICY

This policy is applicable to all pupils, including those in EYFS. Any information specific to a single department will be titled accordingly.

Rationale:

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Mowden Hall with respect to the use of ICT.
- Safeguard and protect the children and staff of Mowden Hall.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Our e–Safety Policy is the responsibility of the Head of ICT. The e–Safety Policy and its implementation will be reviewed annually.

Aims:

- To create and maintain a whole school consistent approach including staff, children and parents.
- To maintain robust reporting routes that are signposted and clear, available to all and provide mechanisms to allow any type of issue to be reported.
- To keep staff, teaching and non-teaching, updated via numerous communication channels including training.
- To integrate e-safety with other policies including behavior, safe-guarding and anti-bullying.
- To integrate with curriculum e-safety teaching especially in Computing and PSHEE.
- To manage the ICT infrastructure to ensure suitable filtering of content is maintained.
- To effectively monitor new developments, risks and ensure e-safety is managed as a dynamic part of the ICT and whole school strategy.

- To manage personal data effectively and in accordance with the Data Protection Act 1998.
- To ensure that any professional communications that utilise technology between the school and pupils, their families or external agencies are:
  - Within clear and explicit professional boundaries
  - Transparent and open to scrutiny
  - Do not share personal information with a child or young person

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Mowden Hall School:

Role	*Key Responsibilities*
Headmaster	• To take overall responsibility for e-safety provision • To ensure the school uses an approved, filtered Internet Service (Barracuda), which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager).

Head of ICT/ e-Safety Co-ordinator	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  ○ sharing of personal data
	  ○ access to illegal / inappropriate materials or sites
	  ○ inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying and use of social media

- To oversee the delivery of the e-safety element of the Computing curriculum
- To report any e-safety related issues that arises, to the Headmaster.
- To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date)
- To ensure the security of the school ICT system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- To ensure the school's policy on Internet Use is applied and updated on a regular basis
- Keeps up to date with the school's e-Safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Teachers

- To embed e-safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)
- To ensure that pupils are aware of research skills and legal issues relating to electronic content such as copyright laws

All staff

- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the e-Safety Coordinator
- To maintain an awareness of current e-safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based

	systems, never through personal mechanisms, e.g. email, text, mobile phones, social media, etc.
Pupils	● Read, understand, sign and adhere to the Acceptable Use Policy ● Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home ● To help the school in the creation/ review of e-safety policies
Parents/carers	● To support the school in promoting e-safety ● To consult with the school if they have any concerns about their children's use of technology

Teaching and learning

Why is Internet use important?

- The Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- Pupils use the Internet outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

The benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;

- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Head of ICT will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole - class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers
- Access in school to external personal email accounts may be blocked.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published
- The Headmaster will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully before publication to the school website (hosted externally) or other social media sites registered by Mowden Hall. Content will never be hosted on any additional external servers except for photos taken by touchline parents at matches, for whom they are responsible, and videos which may appear on the (unlisted) YouTube Channel for Mowden Hall.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites. At the time of writing, access to all social networking sites is prohibited on the school network for all staff and pupils with the exception of Head of Art, Housemistress, Marketing Assistant, Gappies and other staff living in the main building.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends / family, specific interests and clubs, etc.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents / carers, particularly when concerning students' underage use of sites.

Cyber-bullying

- The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.
- The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- If staff or pupils discover unsuitable sites, the URL should be reported to the School e-Safety Coordinator who will then take the appropriate action.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from the Head of ICT.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

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

Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read the School Acceptable Use Policy (in the Mowden Hall Handbook) before using any school ICT resources (see Appendix)
- As a rule, visitors and parents will not be given access to the school's wi-fi network, although exceptions may be made by the Head of ICT in special circumstances
- Parents will be informed that pupils will be provided with Internet access appropriate to their age and ability.

- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- There will always be a member of staff on duty when pupils are allowed access to the Internet.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety Policy is adequate and that the implementation of the e–Safety Policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content, etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and, where appropriate, in any relevant areas e.g. Bullying or Child protection log. The current log can be seen here.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the e-Safety Co-ordinator and escalate the concern to the Police
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety Co-ordinator to communicate it more widely, as may be necessary.

How will e–safety complaints be handled?

- Any complaint about staff misuse will be referred to the Headmaster.
- All e–safety complaints and incidents will be recorded by the school, including any actions taken.

- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Cyberbullying be managed?

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider, if necessary.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

Due to the sensitivities of taking photographs of very young children and the requirement to use cameras to record children's progress, there is a separate policy for Mobile Phones, Technological Devices & Cameras for EYFS. This can be found in the appendices.

- The use of mobile phones is not permitted by pupils at Mowden Hall. All such devices must be handed in by pupils to staff whenever they are brought to school. The same applies to mp3 players (ipods), iPad's and any other device that use the cell network.
- Kindles may be used by pupils for reading purposes only. They must never be given access to the school wi-fi, especially for short term purchasing of books from the Kindle store, as it is important these purchases are only ever made with parental permission. It is therefore important that pupils arrive at school with a Kindle that is pre-stocked with books bought prior to the start of term.
- School staff may confiscate a phone or device if they see them being used by students

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- No electronic devices may be taken into examinations, except for calculators when permitted. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for pupils within or outside of the setting in a professional or personal capacity. There may be occasions when staff use their own personal phones to contact parents, but there is no obligation to do so. A private space will always be made available should a staff member need to contact a parent. In addition, staff must appreciate that using their own phone to contact parents will mean their personal details are potentially made public. All staff using a personal device must ensure it has a lock enabled.
- Mobile phone and devices should be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices should not be used during teaching periods except in emergency circumstances.
- If members of staff have an educational reason to allow children to use personal devices as part of an educational activity then it will only take place when approved by the Headmaster.
- Designated staff are permitted to use personal devices such as mobile phones, iPad's or cameras to take photos or videos of pupils for the purposes of the school website or social media accounts, but good practice dictates that all such data should be deleted from those devices immediately once transferred. Please refer to Appendix C for a list of designated staff. Staff should also be aware that all photos are transferred to the School (Google) drive. Staff should not download or store any images from the drive (or any other school platform) on their personal devices.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Parental Use of Personal Devices

Parents are not covered by the Data Protection Act 1998 if they are taking photographs or making a video recording for their own private use and are therefore at liberty to take photographs or make video recordings at school events. On occasion parents may be publicly asked not to take photographs.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use. Recording and or photographing other than for

private use would require the consent of the other parents whose children may be captured on film.

Parents, staff or visitors who suspect anyone of taking images of children without consent must report the incident to the Designated Safeguarding Lead immediately.

Official School Photographs

Official School Photographs are taken throughout the year by accredited photographers who are DBS checked, fully insured and chaperoned during their time on school premises.

Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme is ongoing across the school to raise the awareness and importance of safe and responsible Internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-safety education will be given where pupils are considered to be vulnerable.

Appendix A

e-Safety References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Safer Internet Day: www.saferinternet.org.uk

Appendix B

School Policies and E-safety Documents

Mobile Phones, Technological Devices & Camera Policy for EYFS

Mowden Hall School recognises that staff may wish to have their personal mobile phones at work in case of emergency. It is acknowledged that staff may also have other technological devices in their possession or within their personal belongings.

However, safeguarding of children within the school is paramount and it is recognised that personal mobile phones and technological devices have the potential to be used inappropriately and therefore the following policy is implemented. It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Mobile Phones

- Mowden Hall School allows staff to bring in personal mobile telephones for their own use.
- Users bringing personal mobile telephones into Mowden Hall School must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephones are left inside their bag throughout contact time with children. Staff bags should be placed in the lockers in the staff cloakroom.
- Mobile phone calls may only be taken during staff breaks or in staff members' own time. If staff have a personal emergency they are free to use the setting's phone or make a personal call from their mobile in an appropriate area. Personal mobile phones and technological devices should only be used outside of working hours and never whilst children are present.
- If a member of staff is waiting for an emergency personal call then their phone may be left with the Head of EYFS who with permission will answer and then notify the member of staff.
- If a staff member, student or volunteer must use their mobile phone (see above) this should be away from the children and ensuring that staff supervision levels are not compromised.
- Staff, students or volunteers who ignore this policy and use a mobile phone on the setting premises without permission may face disciplinary action.
- The school's main telephone number can be used for emergencies by staff or volunteers or by people who need to contact them.
- In circumstances such as outings and off site visits, staff will agree with the head of EYFS the appropriate use of personal mobile phones in the event of an emergency.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Head of EYFS.
- Where there is a suspicion that the material on a mobile phone or technological device may be unsuitable and may constitute evidence relating to a criminal offence. Concerns will be taken seriously, logged and investigated appropriately in line with our safe guarding policy.
- Staff, students or volunteers remain responsible for their own property and will bear the responsibility of any losses.

- Staff will need to ensure that the Office has up to date contact information and that staff make their families, children's schools etc., aware of emergency work telephone numbers. This is the responsibility of the individual staff member.

Use of personal mobile phones, cameras and technological devices by non staff

- Mobile phones are to be left in the lockers in the cloakroom. If it is necessary for non-staff to have their mobile phones to implement their role effectively then they are to be supervised at all times.
- Mobile phones and technological devices must only be used away from the children and where possible, off site.
- Photos of children must not be taken without prior discussion with the Head of EYFS and in accordance with the Data Protection Act and the use of images consent form.
- In circumstances where there is a suspicion that the material on a mobile phone or technological device may be unsuitable and provide evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed (please refer to the 'Child Protection Policy').
- Visitors remain responsible for their own property and will bear the responsibility of any losses.

Use of the School's mobile phone, camera and technological devices

- Mowden Hall School provides mobile phones and cameras for staff to use to support their work with children. To ensure the appropriate use of this equipment, and to safeguard children, the following policy applies.
- Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements and are an effective form or recording their progression in the Early Years Foundation Stage. They may also be used on our website, social media sites, and/or by the local press with permission from the parents.
- However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
- Only the designated Mowden Hall School cameras are to be used to take any photos within the setting or on outings.
- Images taken on this camera must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the location of the cameras, they should be placed within a filing cabinet at the end of the day.
- Images taken and stored on the camera must be downloaded on site as soon as possible, then deleted.
- Under no circumstances must cameras of any kind be taken into the toilet area without prior consultation with the Head of the EYFS.
- If photographs need to be taken in the toilet area i.e. photographs of the children washing their hands, then the Head of EYFS must be asked first and staff to be supervised whilst carrying out this kind of activity. At all times the camera must be placed in a prominent place where it can be seen.

- Only the camera and technological devices belonging to the school may be used to take appropriate and relevant images of children, i.e. observations, photographs of setting events.
- The school's mobile phone must only be used for work related matters.
- The school's mobile phone and technological devices remain the property of the school at all times and should not be taken off of the premises (with the exception of visits and outings).

Productions/Outings

- Photographs maybe taken during productions/outings if permission has been granted by the Head of the Pre-Prep as occasionally there are restrictions for safety reasons. If permission is granted then photographs are only for parental/carers personal use and must not be placed on any social network sites.

Failure to adhere to the contents of this policy will lead to disciplinary/safe guarding procedures being followed.

Appendix C

Designated persons to take photographs of children on personal mobile phones or cameras:

- Senior Management Team
- Marketing staff
- Teaching staff
- Games staff
- Housemistress
- Boarding staff
- Teaching assistants

Members of staff to use school camera for taking photographs

- Gap students
- Other members of staff

Pupil Acceptable Use Policy

Information and Communication Technology
Acceptable Use Policy for Mowden Hall Pupils

Technological solutions are in place in our school to provide a safe and secure environment in which to work. While no solution can be absolutely effective in guaranteeing your safety when using the Internet and related technologies, the solutions we have can help to minimise the risks to you, particularly when supported by clear acceptable forms of use. It is therefore important that you read this document carefully and understand the School's requirements when using the technology at your disposal.

Internet Content Filtering

The School has a content filtering system in place that filters all data received via the Internet. This is in place to prevent inappropriate material being accessed. Content management is carried out by a designated staff member and approved by the Headmaster. It is continually reviewed in order to stay up to date. Within school you may not access the Internet using any private service provider on mobile technology (e.g. iPhone, iPad, Blackberry, iPod Touch, G1 phone, personal laptop, etc.). All internet access within school must be done using the school network system.

Internet Access Monitoring

All internet access is monitored. If you accidently access material that offends or upsets you, you must inform a teacher immediately in order to help prevent this reoccurring. If there has been a deliberate attempt by you to access inappropriate material, or misuse of the School's facilities for non-educational purposes, the Headmaster will be informed. Necessary action will be taken depending on the seriousness of the offence. This could result in the temporary suspension of ICT privileges or permanent exclusion.

Anti-virus Protection

All computers are provided with anti-virus protection. This is reviewed and updated on a regular basis. You should always have the permission of your Head of ICT before copying files to, and removing files from, the School filing systems. Do not use removable media (CD/DVD-ROMs, USB storage and any other mass storage device) on the School computers without the permission of your Head of ICT. Inform a teacher immediately if the anti-virus software alerts you that material you are using is infected. You may not attempt to load any form of software on a workstation. This will be done by the Head of ICT.

Email

All pupils have access to the School email system in order to compliment their educational experience. You may not use an alternate webmail system like Hotmail, Yahoo Mail etc. All incoming and outgoing email will be scanned for viruses and spam (Junk mail). Email will be monitored to ensure your safety and prevent abuse and misuse. If you receive an email that is inappropriate, report it immediately to a teacher. If you deliberately use your email for unsuitable activities, the Headmaster will be informed. Necessary action will be taken, depending on the seriousness of the offence. This could result in the temporary suspension of email privileges to a permanent exclusion of use.

For boarding pupils, it is acknowledged that emails are used for personal communication as well as supporting classroom activities. All mail will still be monitored and scanned in the usual method.

Equipment and Data Security

Measures are taken to help protect your data and the equipment by giving you access rights. You must only use the usernames and passwords given to you by your teachers. Only technological equipment provided by the School may be used to access the School network. Do not attempt to use mobile phones, personal laptops, PDAs or any form of mobile device on the School network unless you have the Headmaster's permission.

Using printers, scanners, data logging equipment, portable storage, photographic and video equipment and any other form of technology, fixed or portable, requires a sensible and responsible user. Do not waste paper or ink/toner when printing. Do not waste time when you have access to the equipment. Do not use any equipment unless you have the permission of a teacher.

Your role and ours

The School believes that using the technological equipment provided will compliment the education you are receiving. We trust that you will understand why measures are in place to control your access to this equipment. Your teachers will discuss any questions or concerns you may have. The School will offer the necessary support for you to have a meaningful and worthwhile experience when using the technological equipment.

I have read the information in this Acceptable Use Policy and understand my responsibilities. I will make every effort to obey the requirements mentioned in this Acceptable Use Policy.

Pupil

Signed: _____ Name: _____

Parent witness

Signed: _____ Date: _____

Staff Acceptable Use Policy

MOWDEN HALL SCHOOL

Information and Communication Technology

Acceptable Use Policy Summary for Mowden Hall Staff
Summarised from the Cothill Educational Trust Handbook - Computer Use Policy (Sect 6.1 to 6.12)

Technological solutions are in place in your workplace to provide a safe and secure environment in which to work. While no solution can be absolutely effective in guaranteeing your safety when using the Internet and related technologies, the solutions we have can help to minimise the risks to you, and our pupils, particularly when supported by clear acceptable forms of use. It is therefore important that you read this document carefully and understand your workplace's requirements when using the technology at your disposal. This serves to summarise, and by no means substitute, the Cothill Trust Handbook – Computer Use Policy (Section 6.1 to 6.12) of which you should be familiar.

- If a user is at all uncertain or unclear about any regulations he or she should discuss them with the Headmaster or Head of ICT before using the School's technological resources.
- Users should observe security measures put in place. Always use usernames and passwords issued to you by your ICT department. Do not leave workstations unattended while logged on.
- Internet and Email access are available for work related matters. Private use of these systems should not impact on your level of productivity and should not put pressure on the IT infrastructure. The School reserves the right to withdraw this facility if the privilege is abused.
- Monitoring and Filtering of your Internet and Email access is done to prevent undesirable content and virus attacks. Your workplace strives to keep up with the latest technologies in this area in order to offer you a safe environment in which to work.
- Downloading and installing material must be approved and monitored by your ICT Department. This will help to keep workstations running efficiently and ensure software licences are monitored.
- Equipment must be kept safe and secure. Lock away portable equipment when in your care. Return equipment to the relevant department when not in use. Keep equipment and data secure when removing it from the school. It must be returned to school as soon as possible.
- Familiarise yourself with the relevant requirements of the Data Protection Act of 1998 especially if you are involved in data processing.
- Help look after the equipment by supervising the use of it when pupils are required to use the technology in your lessons.
- Keep your ICT Department informed if equipment is faulty or not operating correctly. Do not attempt to repair faults unless you have been sanctioned by the ICT Department to do so.

I have read the information in this Acceptable Use Policy Summary and understand my responsibilities. I will comply with the requirements mentioned in this Acceptable Use Policy Summary.

Staff Member Name: _____

Signed: _____ Date: _____