ICT Acceptable Use Policy

Mortimer Primary School
ICT Acceptable Use Policy

All involved parties should read the Acceptable Use Policy to ensure that they fully understand and accept the contents before signing it.

Acceptable and Responsible Use of ICT Resources'

This version was created September 2023 and will be reviewed September 2024.

Declaration

I have read and agreed to the terms and conditions set out in the School's Acceptable Use Policy.

Signed: _____

Date: / /

Contents

1 THE BENEFITS OF INTERNET ACCESS FOR EDUCATION

Most curricula at European level require students to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the Internet offers both students and teachers vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between students from all over the world, while at the same time providing access to educational, social and leisure resources.

The main reason that we provide Internet access to our teachers and students is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Unfortunately, as there is the possibility that students will encounter inappropriate material on the Internet, the school will actively take all reasonable precautions to restrict student access to both undesirable and illegal material.

Teachers are responsible for guiding students in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that students are only too aware of what is regarded as acceptable and responsible use of the Internet. The main goal is to utilise Internet access to enrich and extend those learning activities that reflect the curriculum requirements and the age and maturity of the students.

Students will access suggested websites by their teacher. These will have been previewed and approved by their teacher whenever possible.

The free use of search engines is permitted only with Key Stage 2 pupils and when using child friendly search engines, for example *Swiggle,* can filter most websites with inappropriate content and will be used as a first option. Other search engines intended for use by students offer a filtered list of links. The Local Authority firewall will also act as a safeguarding tool and any breaches of security must be reported to the head teacher or a member of the senior leadership team.

All Internet access is filtered through a proxy server to screen out undesirable sites at source. Any inappropriate material, such as images or text, should be reported to the Computing Lead (Miss A. Marshall) who will then report to technical support for the website to be added to the blocked list.

2 WHOLE-SCHOOL NETWORK SECURITY STRATEGIES

The school's computer network security systems are reviewed regularly by our technicians.

Uploading and downloading of non-approved application software is denied. All access to the school network requires entry of a recognised User ID and password. Students and staff must log out after every network session.

Virus protection software (Smoothwall Monitor) is installed and updated automatically daily. Teacher laptops should be turned off fully each evening and then restarted each morning to 'pick up' the new updates. It is the teachers responsibility to do this.

Using personal hard drives, USB sticks and memory devices on the school network requires specific teacher permission and a virus check. The preferred method of storage is Google Drive, this is cloud based storage.

Unapproved system utilities software and executable files are not allowed to be stored in student storage areas.

Student files held on the school's network are available to be checked by staff with approved access.

Hardware and software infrastructures

The school has invested in the following hardware and software infrastructures to reduce risks associated with the Internet.

IDex Client – an application which forwards usernames, group membership, and information about web requests to the Smoothwall Filter and Firewall for web filtering purposes.

Client Server network – in conjunction with an information and web management system

Filtering Software

Firewall – that has been configured to prevent access to inappropriate websites.

Smoothwall Monitor – External monitoring for key words and images on all staff and pupil devices.

Classroom management structures

- Ensure that computers/chrome books are positioned in such a way that monitors are easily observed by teachers wherever possible. Children should not have unsupervised access to those computers with internet access.
- When using iPads, Apple Classroom should be initiated and the teacher should be using the teacher console to monitor usage.
- When using laptops/chrome books, Google Classroom can allow pupils to share their work with the teacher and the teacher can monitor the work being produced in 'real time' and also the websites being accessed through the use of Impero.

3 RISK ASSESSMENT AND MANAGEMENT OF INTERNET CONTENT

The school has taken and will continue to take all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked computer. The school, however, cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

All students are taught effective online research techniques, including the use of subject catalogues and search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received;
- Using alternative sources of information for comparison purposes;
- Respecting copyright and intellectual property rights.

Students will be made aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as violence, racism and exploitation of children.

However, if they do encounter such material, they will know that they should minimise the screen whether it be a laptop, chrome book or iPad, not turn off the device, and report the incident to the nearest teacher or the school's Computing Coordinator who will deal with it according to the school Acceptable Use Policy.

4 REGULATION AND GUIDELINES

The school's Internet access incorporates a software filtering system to block chat rooms, newsgroups, social media sites and inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate sites is blocked.
- Access will be allowed only to a listed range of approved sites.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- A rating system is used to rate web pages for inappropriate content and that the web browsers are set to reject these pages.

Accessing a site denied by the filtering system will result in a report being generated and sent to the LEA administrator. The school's Head Teacher and Computing Coordinator regularly assesses the effectiveness of the filtering system.

The school will immediately report the details of any inappropriate *or* illegal Internet material found to the LEA through ICT in Schools at The Word.

Similarly, the school will request Mike Hamilton to 'allow' access to certain banned sites and provide the educational reasons behind the request. They can only be requested and approved when an application is made by a member of the Senior Leadership Team.

4.1 Email accounts

Students may only use their approved email account/s on the school network during school time or at home under parental supervision when using Google Classroom. The email system currently allows children only to email other students and members of staff. However, staff and children are not advised to communicate via email. All communication should be open and if necessary through the stream on the Google Classroom. This should only be a port of contact when learning about email as a function.

Staff and students shall immediately report any offensive emails that they receive to the Computing Lead or their teacher.

Access in school to external, Web-based, personal email accounts, eg. Hotmail is denied for network security reasons.

Staff and students must read their emails regularly and remove superfluous emails from the server.

Students may not reveal their own or other people’s personal details; such as addresses or telephone numbers or arrange to meet someone outside school via the school network.

Sending and receiving email attachments is subject to permission from the teacher.

If a child or teacher needs to contact each other, this should be via ‘The Stream’ on Google Classroom. Teachers may post a private a message to a particular child through the Classroom stream settings. As there are other members of staff in every classroom they will be able to see and be there as chaperones for communication. The teacher must start the post with, “This is a post for you only, it is visible by only the members of staff in this group and yourself.”

This form of communication is generally only required during periods of remote learning.

4.2 The school's website

The School Leadership Team and Computing Lead manages all aspects of placing web pages on the school's website. It has full editorial responsibility and ensures that the content on the site is accurate and appropriate. The website will comply with the Education Authority's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, email address and telephone number. No information about teachers' or governors' home addresses or the like will be published.

The school will not publish any material produced by students without the agreed permission of their parents. In addition, photographs of students will not be published without a parent or carer's written permission. A student's name will not be used in association with photographs.

Website photographs that include students will be carefully selected and will be of a type that doesn't allow individual students to be identified by name.

4.3 Moderated mailing lists, newsgroups and chat rooms

The school uses an email distribution list to send messages to selected groups of users. Children will only be permitted to use their email account hosted by Real Smart, accessible through the website to communicate via email during school time.

Students will be denied access to public or unmoderated chat rooms.

Only regulated educational chat environments shall be used. They will always be used under supervision. Safety is the major consideration.

4.4 Other communication technologies

Students are not allowed to use mobile devices during lessons or formal school time. This also includes the use of cellular Smart Watches or any other smart watch which can connect to the Internet or take photographs. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network.

All students must turn off their devices before entering the school yard; phones must be given to the teacher at the start of the day for safekeeping and will only be returned at the end of the day. Phones must remain turned off until students have left the school yard.

If a pupil is found with a device in school (including in the playground) without permission the device will be taken from the pupil and placed in the school office. Parents will be contacted and asked to collect the device in person.

If a pupil is found using a device on the school site for any purpose including messaging, taking photos or video, this will be regarded as a serious offence and the Head Teacher will decide on appropriate action.

Parents are advised that Mortimer accepts no liability for loss of or damage to mobile phones which are brought into the school. It is the responsibility of the parents and pupils to ensure mobile phones are adequately insured.

If a pupil needs to contact his/her parent/guardian they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly.

Further action will be taken if mobile phones are used and there are child protection implications as in line with “Keeping Children Safe in Education” (2023). The severity of the action from the school will depend on the particular circumstances. Appropriate external authorities will be alerted if necessary including Social Services and Police.

Staff mobile phones and personal digital devices

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

Staff **will not** use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use

work-provided equipment for this purpose.

Staff **will not** use any personal devices directly with children and will only use work-provided equipment during lessons when on site. Staff may use their own personal mobile phone, as a means of communicating with school, when on extra-curricular visits but must inform the office of their number.

Staff personal mobile phones and devices **must be** switched off/switched to 'silent' mode during lesson times. Mobile phones may be accessed during non-teaching times but must only be accessed when children are not present and not in corridors or practical areas and out of eyesight and hearing distance of pupils.

Personal mobile phones or devices **must not** be used during teaching periods.

When checking mobile school emails on mobile devices, staff must ensure that children are not present.

Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.

If a member of staff breaches the school/setting policy then disciplinary action will be taken.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

Staff **should not** attach their personal devices to the Wi-Fi system in school.

4.5 Visitors use of personal devices and mobile phones

Parents/guardians and visitors must use mobile phones and personal devices in accordance with the ICT Acceptable Use Policy.

Parents/guardians/visitors may use their mobile phones, only when permission has been granted by the Head Teacher or teacher in charge, during school performances. Parents/guardians/visitors should be mindful and only take pictures of their own child. Any photos or videos taken **must not** be placed on social media or distributed to a third party which contain children other than their own without the permission of the

other child's parent/guardian.

If a parent/guardian/visitor has permission to be on site of the school, they must not use their mobile device while walking around the school to call, take photos or use any of its other features. It should be turned to silent on entering the school so as to not disturb children when working.

If an adult is seen using a mobile phone a member of staff will ask them to end the call or if a photo has been taken a senior member of the leadership team will be informed and the adult may be asked to delete the picture/video.

Adults accompanying trips must not take photos or videos of children using their own mobile phones or own personal camera.

If an adult requires to use a mobile phone during a trip or residential visit they must do so discreetly and with the agreement of the trip leader.

4.6 Laptops/iPads

Staff and student teachers provided with a laptop / iPad purchased by the school can only use it for private purposes at the discretion of the Head Teacher. Such laptops / iPads remain the property of the school and are open to scrutiny by senior management, contracted technicians and the Computing Lead.

Laptop / iPads belonging to the school must have updated antivirus software installed and be password protected. This will be updated regularly through updates pushed out from the school technical team and remotely from Smoothwall Monitor. Members of staff must turn off devices fully regularly as updates are received when a device is restarted.

Staff intending to bring personal laptops / iPads onto the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop / iPad.

Staff should not attach personal laptops / iPads to the school network.

The security of school laptops / iPads is of prime importance due to their portable nature and them being susceptible to theft.

Students and visitors to the school should not be given the wi-fi password to use on their own personal devices unless granted permission by a

member of the Senior Leadership Team.

(See attached appendix Laptop/iPad Policy for Staff)

4.7 Handling online safety complaints

Any online safety complaint will be dealt with in line with the school complaints policy.

Any complaint about staff misuse must be referred to the Head Teacher who will decide if sanctions are to be imposed.

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

In correlation with Keeping Children Safe in Education 2023, all staff have a responsibility to provide a safe environment in which children can learn. Any staff member who has any concerns about a child's welfare should follow school protocols and inform DSL or an appropriate member of the Senior Leadership Team.

The Head Teacher will arrange contact/discussions with South Tyneside Local Authorities and the police to establish clear procedures for handling potentially illegal issues.

4.8 Cyberbullying

Cyber bullying will not be tolerated in school. Details of how bullying incidents are managed are set out in the school's Anti-Bullying Policy.

All incidents of Cyberbullying reported to the school will be recorded by a member of the senior leadership team and a CPOM should be recorded by adults involved in the situation.

The school will take steps to identify the perpetrator where possible, such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the police if appropriate.

If this is an incident reported by parents that has happened external to school, that is preventing a child wanting to attend school and/or involving other pupils, DSL will be informed, if deemed necessary the incident will

be recorded, appropriate evidence stored and if necessary actions taken by the school. If this is of a more serious nature, then this may be shared with external organisations.

Parents/guardians will be informed.

All staff should be aware of *Keeping Children Safe in Education 2023* and key signs and triggers to be aware of. All staff should be aware of the school's policy and procedures regarding peer on peer abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

Child-on-child cyber bullying is most likely to include, but may not be limited to:

- Bullying (including cyber bullying, prejudice-based and discriminatory bullying)
- Sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse. (p.12)
- Censual and non-consensual sharing of nude and semi-nude images and/or videos.
- Up skirting which typically involves taking a picture under a person's clothing without permission.
- Initiation/hazing type violence and ritual. This could involve activities involving harassment, abuse and humiliation used as a way of initiating a person into a group and may also include online elements.

4.9 Use of Social Media for staff

Staff members will not accept friend requests from current pupils, or ex pupils under the age of 18 on social media sites.

No member of staff should use social media to correspond with parents on school related matters other than on the open Mortimer Primary School facebook page. Staff should not discuss school concerns or queries through direct messaging on social media.

No member of staff must discuss school related topics including pupils and other staff members on social media other than on the school social media pages. All comments made must be in line with school policy and opinion and not that of the opinion of the staff member.

Office email or the school phone number should be the only modes other than direct face-to-face contact used.

Photos of school events, trips and residential visits should not be posted on personal social media accounts. **This includes pictures taken by staff members inside the school building or on site from themed days and events.**

All members of staff who use social media sites are encouraged to use the tightest privacy settings possible. Staff are reminded not to post their place of work in personal information on their social media.

Social media sites must not be accessed on school devices on school premises.

Any complaint about staff misuse must be referred to the Head Teacher who will decide if sanctions are to be imposed.

Staff must not place a child at risk of harm.

- Staff must follow statutory and school safeguarding procedures at all times when using social media.
- Staff must report all situations where any child is at potential risk by using relevant statutory and school child protection procedures.
- Staff must not allow their use of social media to affect their ability to do their job in any way.

Social media relationships must be declared with other personal relationships or interests whenever necessary or appropriate.

Staff must maintain the reputation of the school, its staff, its pupils, its parents, its governors, its wider community and their employers.

Staff must not contribute or access any social media content which is illegal, discriminatory, sexual, or otherwise offensive when linked in any way to the school. This link could be, as examples, by identification with the school, during the working day, on school premises or when using school equipment. Such behaviours may also result in criminal proceedings.

Staff must recognise that contributing or accessing any social media content which is illegal, discriminatory, sexual or otherwise offensive during personal use could lead to damage to their professional reputation or damage to the reputation of the school. This damage would breach the social media policy. And, again, such behaviours may also result in criminal proceedings.

Staff must not use social media to criticise or insult their school, its staff, its pupils, its parents, its governors or its wider community.

Staff must not use social media to harass, bully or intimidate any pupil, parent, member of staff, governor or other member of the wider school community.

Staff **must not** breach school confidentiality.

School staff must follow their school data protection responsibilities when using social media.

Staff are responsible for their actions (and its consequences) whenever they use social media.

- Staff are responsible for all their social media content.
- Staff must understand that social media offers no guarantee of privacy and that any content they produce can be shared more widely by others. A staff's professional reputation or the reputation of the school could be damaged by content, perhaps which was intended to be private, being shared more widely than intended. It is the responsibility of the staff member to control their own social media.
- Staff would still be held responsible for any consequential breach of this policy as they were responsible for producing the original content.
- Staff are responsible for the configuration and use of any personal social media accounts they have. They are responsible for determining the level of security and privacy of all their social media content.
- Staff must raise all doubts, questions and concerns related to social media with school leaders. Staff must seek advice if they are not sure if any particular use of social media (or a related action) is appropriate or would potentially breach this policy. **Staff cannot rely on their ignorance or lack of knowledge to defend any breach of this policy.**

When using social media in staff's wider professional life

- Staff must be clear that their social media content is personal and not endorsed or supported by their school.

- Staff cannot use account names, school branding or anything else that could imply that the content is official school content. They are encouraged to not name their school in any posts.

- Staff must be particularly careful to not reveal any details of staff, pupils, parents or other members of the school community that make it possible to identify any individuals.

- Staff must use appropriate behaviour and language at all times. As a guide, this should be similar to that which would be used when taking part in a face-to-face meeting with other education professionals.

- Staff **must not** state on their social media that they work at Mortimer Primary School or are an employee of South Tyneside Council.

When using social media in staff's personal life

- The personal use of social media must neither interfere with a member of staff's ability to maintain their professional reputation nor impact on the reputation of the school.
- Staff must take all reasonable steps to ensure the proper separation of their professional and personal lives.
- Staff must not use school social networking accounts for personal content.
- Staff must respect the wishes and privacy of any other members of their school community with whom they have personal social media contact.

Staff must not use personal social media with anyone with whom they solely have a staff/parent relationship.

- Staff at schools can often have more complex relationships than just being a member of staff or a parent. As examples, staff can also be parents (of pupils at the school), in relationships or have friendships with other staff or parents or also governors. Any member of staff should report any social media relationships to senior leaders for their own protection.

- Staff must make sure that their personal social media activities take into account who they have social media relationships with – particularly any other members of the school community – and moderate their social media behaviour accordingly.

4.10 Pupil use of Social Media

All pupils in our school will be reminded frequently and regularly that they are below the permitted age to join many social media groups. (13 for most sites including Facebook, Snapchat, Tik Tok and Instagram.)

Parents will be informed if a child is found to be using a site that is inappropriate for their age in a dangerous manner or inappropriate way.

Teachers/parents/guardians/pupils will be informed how to report abuse and inappropriate content.

Any child who is reported to have made inappropriate comments (including private messages) about the school, pupil or member of staff will be reported to the Head Teacher who will decide if sanctions are to be imposed.

4.11 Use of Social Media for parents/guardians of the School

Parents/guardians **must not** post photos, videos or comments that include other children at the school.

Parents/guardians **must not** use social media on their own devices while on school premises or helping on educational trips.

Parents/guardians are encouraged to raise queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents to communicate with each other) or on the school's pages

Parents/guardians must not post anything malicious or of a threatening nature about the school or any member of the school community. Anything that is reported to the school will be taken seriously and the Head Teacher will decide what sanctions are to be imposed.

4.12 Keeping Children Safe in Education 2023 and Digital Responsibilities:

All staff and parents/carers/guardians should be aware that technology is a significant component in safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face.

In many cases abuse will take place concurrently via online channels and in daily life.

Children can also abuse their peers online, this can take the form of abusive harassing, misogynistic messages, non-consensual sharing of indecent images, especially around group chats and sharing of abusive images and pornography to those who do now want to receive it.

Child-on-child abuse is most likely to include, but may not be limited to:

- Bullying (including cyber bullying, prejudice-based and discriminatory bullying).
- Sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse.
- Censual and non-consensual sharing of nude and semi-nude images and/or videos.
- Up skirting which typically involves taking a picture under a person's clothing without permission.
- Initiation/hazing type violence and ritual. This could involve activities involving harassment, abuse and humiliation used as a way of initiating a person into a group and may also include online elements.

School Actions:

- All staff will receive termly updates and training. Staff are aware and follow KCSIE 2023 guidelines and will liaise with the Designated Safeguard Lead (Mrs Peacock) if and when they have any concerns.
- Parents will receive regular online safety updates.
- Parent Online Safety Awareness meetings will be delivered by the Computing Lead and other agencies.
- Children from Nursery to Year 6 receive age appropriate online safety lessons and Reception to Year 6 participate in KidSafe, age appropriate sessions that discuss and remind children what to do in dangerous and uncomfortable situations. Highlighting the emphasis to say no, walk away and tell a trusted adult.

Cybercrime:

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either ‘cyber enables’ (Crimes that can happen offline but are enabled at a scale of speed on-line) or ‘cyber dependent’ (crimes that can be committed only by using a computer.) Cyber dependent crimes include:

- Unauthorised access to computers (illegal hacking) for example accessing a school's computer network or website to look for test paper answers or to change grades awarded.
- Denial of service (Dos or DDoS) attacks or ‘booting’. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources.
- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets, and Remote Access Trojans with the intent to commit further offence, including those above.

School Actions:

- Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the DSL should consider referring into the Cyber Choices programme.
- Any adults found to/ believed to be committing cybercrimes will be reported to the head teacher who will decide the further actions to take.

Adults working in school are reminded that they should always log out of/lock their device when leaving the room. If when using your device, you believe something has changed, altered, the computer may be running slower then to seek technical support straight away and stop using the device.

5 COMMUNICATING THE SCHOOL’S ACCEPTABLE USE POLICY

5.1 Informing students

Students will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet. The ‘Pupil version of the Acceptable Use Policy’ will be shared with pupils via their teachers.

5.2 Informing staff

All staff will be provided with a copy of the School's Acceptable Use Policy. Teachers are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted regularly about the development of the school's Acceptable Use Policy and instructions on safe and responsible Internet. Teachers will also sign the relevant part of the Acceptable Use Policy' document.

To avoid misunderstandings, teachers will contact the Senior Leadership Team regarding any doubts that arise concerning the legitimacy of any given instance of Internet use.

5.3 Informing parents / carers

Parents' attention will be drawn to the School Acceptable Use Policy during parent digital awareness workshops, in the school newsletter, in the school brochure and on the school's website. Advice that accords with acceptable and responsible internet use by students at home will be made available to parents. Safety issues will be handled sensitively.

The school will obtain parental consent before publication of students' photographs.

All comments on and suggestions concerning this Acceptable Use Policy should be sent to the Head Teacher.

Appendix 1
Laptop / iPad Policy for Staff

Staff provided with a laptop / iPad purchased by the school, agree to the following terms of use:

1. The laptop/ chrome book / iPad remains the property of Mortimer Primary School and is for the use of the person it is issued to and must be returned to the school if and when the teacher leaves employment at the school.

2. The laptop/ chrome book / iPad is open to scrutiny by senior management, contracted technicians and the ICT Subject Leader at school.

3. Acceptable Use – teachers should accept and adhere to the school's Acceptable Use Policy, particularly with regard to Internet access.

4. The loading of additional software must be authorised by the school support teaching and learning and be compliant with the following regulations:

   Copyright, Designs and Patents Act 1988

   Specifies that all software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.

   Computer Misuse Act 1990

   Identifies three main offences concerning unauthorised access to systems, software or data.

   If you are in any doubt, please speak to the Computing Lead / Head teacher before loading any software.

5. Anti-Virus software must be installed and should be updated on a regular basis.

   School IT staff will advise on the routines and schedule of this operation. Sophos anti-virus updates are available from school and are covered by the Local Authority license.

6. Members of staff are responsible for updating and maintaining the antivirus software at home.

7. Data Protection – the terms of the school's Data Protection registration should be adhered to and users must clearly understand that there is a personal legal duty on them as well as the school.

8. Any charges incurred by users accessing the Internet from home are not chargeable to the school.

9. Staff should not connect personal laptops / iPads onto the school network.

10. Failure to comply with these guidelines and the school's Acceptable Use Policy, may result in the withdrawal of the laptop / iPad and may lead to disciplinary proceedings.

Laptop & iPad Use Agreement
Standard Terms and Condition of Use

1.1 I agree that the laptop/chrome book/iPad at all times remains the property of Mortimer Primary School and that the laptop/iPad is provided for my use as a teacher: to assist me in developing educational learning materials, for classes taught in the school and to fulfil the administrative tasks my role may require.

1.2 I may use the laptop/iPad for the period of employment at Mortimer Primary School, or until such time as its return is requested by the school, should that happen sooner.

1.3 I understand to keep the laptop/iPad in good working order and to notify the school ICT Support Team i.e. the technical staff, of any defect or malfunction of the laptop.

1.4 I will not engage the services of a third party repair agent for any repairs or maintenance that may be required during the period in which the laptop/iPad is in my care, nor will I tackle any upgrades or repairs myself unless advised by the school.

1.5 I will use the laptop/iPad lawfully and in accordance with Mortimer Primary School's Acceptable Use Policy which may change from time to time, regarding ethical use of the technology, use of the legal software, use of the internet and protection of personal data (ensuring its privacy security at all times.)

1.6 I will not sell, assign, transfer or otherwise dispose of the laptop/iPad.

1.7 If my employment status changes with Mortimer Primary School, or if I breach any of these terms and conditions, the school may revoke this arrangement by giving me a written notice.

1.8 I will return the laptop/iPad to the school in good working order before ceasing to be employed by the school, or upon an earlier date if requested by the school.

1.9 I will take due care of the laptop/iPad package at all times, including:

1. Not leaving the laptop/iPad unattended in a public place.

2. Not leaving the laptop/iPad unattended or unsecured in a classroom or other place in the school, ideally using a locked cupboard/drawer in a locked classroom.

3. Not leaving the laptop/iPad in plain view in an unattended or unsecured vehicle.

4. Not allowing the laptop/iPad to be accessed by any other person (unless authorised by Mortimer Primary School).

5. Not allowing the laptop/iPad to be interfered with, tampered with or altered by a third party, or otherwise, except in accordance with clause 1.3.

6. Ensuring due care is taken in the handling, transporting and usage of the laptop/iPad.

    6.1 I will not remove, conceal or alter any laptop/iPad markings, tags or plates or engrave or mark the laptop/iPad in any way that will reduce the value of the laptop/iPad.

    6.2 If the laptop/iPad is lost, stolen or damaged I will advise the school's Finance Manager and/or Computing Lead and the Police as soon as possible.

    6.3 I will not allow my laptop/iPad or network user account and passwords to be used by anyone other than myself, unless required by the school or technical staff.

    6.4 I understand that due to current software licence agreements covering home use, the laptop/iPad and its software cannot be used by me for any commercial purpose or personal financial gain.