MANSTON PRIMARY SCHOOL

Manston

ACCEPTABLE USE POLICY

Manston Primary is committed to safeguarding and promoting the well-being of all children and expects our staff and volunteers to share this commitment.

Policy reviewed by: James Clay, Karen Cartwright and Kirsty Thorpe
Date: May 2024 Review Date: September 2025

Leeds CITY COUNCIL

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote child achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials

- Educational and cultural exchanges between children worldwide
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The statutory computing curriculum requires children to learn how to locate, retrieve and exchange information using digital technologies. Consequently, in delivering the curriculum teachers need to plan to integrate the use of digital technologies and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

This policy has been produced to encourage and promote the above, and should be read in conjunction with other relevant school policies and national guidance, including:

- Manston Primary's Safeguarding and Child Protection Policy,
- Manston Primary's Online Safety Policy,
- Guide to Safer Worker Practice Guidance, and
- Manston Primary's Behaviour Policy.

1. Aims

Manston Primary aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Have clear user agreements of acceptable use of internet and digital technologies for pupils (appendix 1), staff/volunteers/site visitors etc (appendix 2) and governors (appendix 3)
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' but is not restricted to these). Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The Aims of this Acceptable Use Policy are to:-

- Allow all users access to school digital resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and children are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990, The Data Protection Act 2018 (including the implementation of the General Data Protection Regulation (GDPR) and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in and out of school (such as home learning devices), which are consistent with the general policies of the school.

2. Application

This policy applies to the school governing body, all teaching and other staff, external contractors providing services on behalf of the school or the council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as Outlook, Arbor and CPOMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work. This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people

The 4 key categories of risk:

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

3. Access

Access to the school's network and use of digital facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy.

3.1 School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it will not normally be used to communicate with parents and pupils. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to email parents outside of normal school hours.

3.3 Access to certain software packages and systems (e.g. HCC intranet; SAP (HR, finance and procurement system), Arbor, RAISE Online, FFT, Insight, remote access) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is password protected, always shut down when not in use off site and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

3.5 Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff. If pupils or staff are to be recorded as part of a video conference then they (and their parents/carers) should be informed of this in advance.

3.6 If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

Mobile Devices

Children are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the class teacher to look after during the school day and collected at the end of the day.

Children may not make personal calls or send or receive email or text messages from or to a mobile phone during the school day. Mobile phones may not be used to take pictures of children and staff. Children should not send or receive email or text messages to/from their mobile device during the school day. Any child who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day. Any inappropriate use of mobile devices such as cyber bullying must be reported to the Head Teacher.

Staff should only use their mobile phones at appropriate times of the day only e.g. break times. Normally, during the school day their mobiles should be turned off or set to silent. It should be noted that due to current COVID-19 guidance, staff are permitted to keep phones switched/on their person so they can be contacted in case of household illness or by track and trace – this is in line with the schools safeguarding addendum and the latest KCSiE. When this is updated, this AUP Policy will also be updated. Staff must not use personal mobile devices or cameras to take images of children or staff.

3.7 No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

3.8 Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

3.9 The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4. Communication with parents, pupils and governors

4.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

4.1.2 Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

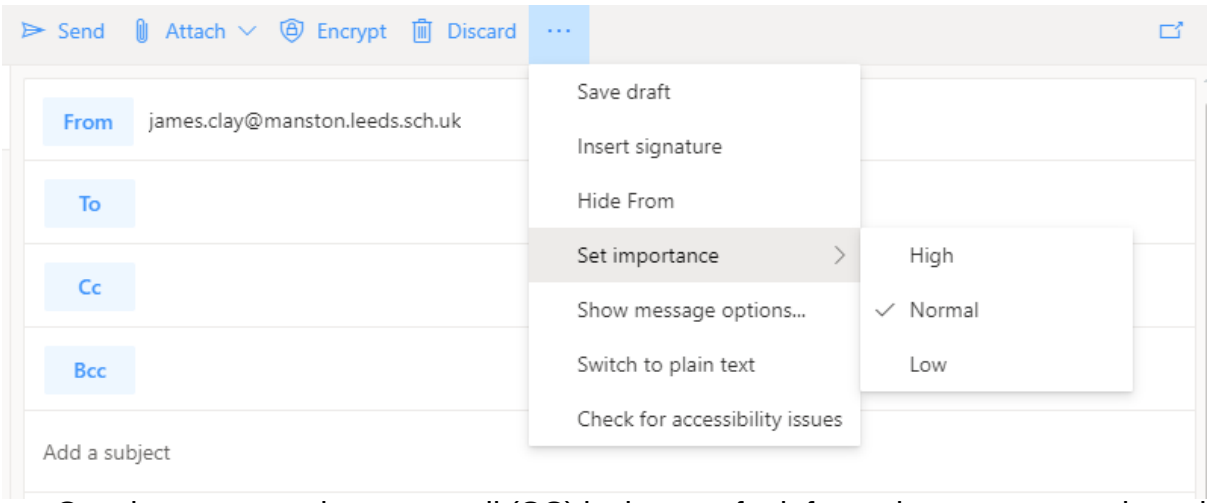
4.1.3 Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Headteacher before sending. Where office staff send letters home these will normally require approval by the Headteacher.

4.1.4 Email – school email accounts should not routinely be used for communication with parents outside school hours. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email. Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

Sending/Replying to staff Emails

- At Manston Primary we promote a healthy work life balance for all staff and want to empower our staff to make the most of communication methods such as email while also promoting staff wellbeing. The below agreement has been drawn up after consultation with staff.
- For a range of reasons many of our staff prefer to work at different times that suit their individual circumstances. In light of this, school will not set times that emails should or should not be sent. However, the following is agreed:
    - Staff are not expected to check their emails outside of working hours
    - Staff are not expected to reply to emails outside of working hours

- Any emails requiring an urgent response will be marked as high importance



- Copying someone into an email (CC) is done so for information purposes only and will not require any action on the recipient's part
- Emails are sent only to the appropriate recipients with large group emails avoided if possible (avoid reply to all emails unless necessary)
- Emails to pupils will always be copied (CC) to the Head Teacher and/or class teacher

When using e-mail, children and staff should:

- Be aware that e-mail is not a completely secure form of communication and therefore children should not send ANY personal information
- Not attach large files
- Not forward e-mail messages onto others unless the sender's permission is first obtained
- Not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive
- Not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated

This Guidance will apply to any inter-computer transaction, be it through web services, chat rooms, bulletin and news groups, blogging or peer to peer sharing

Deletion of staff Emails

- Staff are required to keep their emails in an orderly fashion so that important or urgent information can be accessed with ease.
- Staff are asked and reminded regularly to delete their sent items and delete old emails. Caving any important emails into folders for later use.
- School staff should be aware that school can reinstate deleted emails if this becomes necessary for a specific reason such as: safeguarding, business continuity, record keeping etc.

4.2 Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

5. Social Media

5.1 School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

5.2 Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6. Unacceptable Use

General Internet Use and Consent

Children who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material. The use of the names of children or photographs of children for websites will require written permission from parent(s)/carer(s). If a picture is placed on the website, the child's full name will not be displayed.

Children must not use the school digital facilities without the supervision of a member of staff. Although use of the digital facilities and access to the Internet will be supervised and all possible measures will be taken, Manston Primary School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or children discover unsuitable sites, the URL (address) and content must be reported to a senior member of staff immediately who will, in turn, record the address and report on to the Head Teacher and Internet Service Provider.

Children are aware that they must only access those services they have been given permission to use. Staff and children are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990). Children and parent(s)/carer(s) agree to the Home School Agreement and Acceptable Use Agreement on entry to the school.

General Safety and Risk Assessment

Users must treat equipment and services in school and at other sites accessed through school facilities with respect and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities. Staff are responsible for sharing the safety issues with their children.

Log in and Passwords

- Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Children and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

- Staff and children must ensure terminals or laptops are locked, logged off (or hibernated) or turned off when left unattended. Offsite, all staff laptops must be fully shut down when unattended to activate the Bitlocker encryption system upon reopening/restarting again.

Adult users are expected to oversee their own areas on the network where relevant. Passwords are therefore set for each user in these circumstances. We recommend that passwords are changed regularly. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces. Remember – passwords are case sensitive. „PASSWORD" is different to „password". To protect Manston Primary School's Acceptable use policy, do not tell anyone your password. The password is displayed on screen as a line of ******, however, people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful.

School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share
- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally
- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment
- to collect or store personal information about others without direct reference to The Data Protection Act
- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project
- to use the school's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

6.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

6.3 Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Headteacher or other member of the senior leadership team. Our school uses appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or

facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

6.4 Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

7.0 Personal and private use

7.1 All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the school
- detrimental to the education or welfare of pupils at the school

7.2 It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

7.3 Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

7.4 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

8. Whistleblowing and Cyber Bullying

Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

8.1 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher

where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support Line (02380 626606) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day
- People who cyber bully may attempt to remain anonymous
- Anyone of any age can cyber bully
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient or statements made where the meaning is unclear due to a lack of context or expression.
- Some incidents of cyber bullying can be part of a wider friendship issue
- Cyber bullying is not always directed one way with a victim and perpetrator

8.2 Prevention

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe practice into all our teaching and learning, incidents can be avoided. We recognise that we have a shared responsibility to prevent incidents of cyber bullying. The Head Teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

8.3 Understanding Cyber bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use digital technologies safely. ICT safety is integral to teaching and learning practice in the school.

8.4 Record Keeping and Monitoring Safe Practice

Records of cyber bullying will be kept using the schools CPOMS system for which Cyber Bullying has a specific category. Incidents of cyber bullying will be followed up using Manston Primary School's behaviour procedures.

9. E-Safety

9.1 E-Safety is recognised as an essential aspect of Computing leadership and the Head Teacher, aims to embed safe practices into the culture of the school. The overall responsibility for E-Safety has been designated to our Head Teacher working in conjunction with the Computing Leader and SENDCo.

9.2 All Staff (all teachers, supply staff and teaching partners) are updated of any safety matters. Children are regularly informed about e-safety through planned whole school and class assemblies and as an ongoing aspect of the computing curriculum. Whole school E-Safety

assemblies are held at least annually, with phase assemblies held half termly. These often link to safer internet week, classwork and the schools ongoing work on online safety. The point of these is to reinforce knowledge and understanding; build pupils skills; and reinforce key messages.

9.3 Any work or activity on the Internet using school equipment must be directly related to schoolwork. Private use of the Internet (including social networking sites), as well as using school home learning devices for purposes other than school work and/or homework is strictly forbidden.

10. Other

10.1 All home learning devices will be cleared of any stored passwords and/or data relating to the previous user once they are returned to school.

10.2 If staff are members of social networking sites they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/children or ex-children) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises child or staff confidentiality will be classed as a disciplinary matter.

10.3 Users must not give out personal email, postal addresses, telephone / fax numbers of any person. Under no circumstances give email or postal addresses / telephone numbers / fax numbers of any teachers or children at school.

10.4 Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by children and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

10.5 Users must not download, use or upload any material that is subject to copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material. Users should assume that ALL software is subject to copyright restrictions, including shareware.

10.6 Children must not, under any circumstances download or attempt to install any software on the school computers or tablets. Staff should seek the advice of the ICT technician or the Computing Leader before attempting to download or upload software. Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this or any materials, users must ask teachers or Computing Leader. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

10.7 All children are aware of procedures to report any incidents of sexual or inappropriate content, radicalisation, extremism or anything else that worries them which they encounter during use of the internet. Please see the latest version of the school's Safeguarding policy for details of this. Manston Primary School will react appropriately and work with children, parents and any other appropriate authority to resolve the issue.

11. School Network and Child Files

- Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Where provision allows, children can access and save work to their own log-on through the server; this can only be accessed by that child, the class teacher, the Computing Leader and the ICT technician.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT technician will view any material children store on the school's computers, or on memory sticks/disks children use on the school's computers. Any external storage drives brought in by children must be scanned for viruses before use.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year
- Users accessing software or any services available through school facilities must comply with license agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network or internet is accessed from home, this Acceptable Use Policy applies.
- Where a virtual network (Office 365 such as SharePoint, CPOMS or Arbor) are accessed from home, this Acceptable Use Policy applies.

11.1 Network Security Guidelines

Backups

Where provisions allow, files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup may not be available to restore these.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). No matter how reliable a network is, problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost.

Use your Network Area or Cloud Storage

Staff should look to save documents on their individual One Drive or the appropriate School Share Point sites. If necessary staff can share files in to their own network drive. Staff should NOT save data on the local hard drive. This will mean that your work is backed up and can more likely be retrieved in the event of a hardware failure or theft.

Home Documents

The school cannot accept responsibility for personal documents held on school laptops, it is the responsibility of the user to backup documents created at home or stored on the Home Docs of the laptop.

Off-site child data and child information

Laptops and back-ups (USB sticks/external hard drives) may be taken off site where agreed with the Computing Leader or Head Teacher. Staff are to ensure that laptops are used cautiously when viewing child data/information and images and that laptops are **shut down** -. GDPR 2018 regulations state you must shut down devices when offsite so an encrypted password is required to log back into said device. Images must be transferred to the school network as soon as possible and be removed from mobile devices regularly. Data, images and child information must be removed from backups and laptops when children transfer to another class to avoid records being kept of children that are not taught by their former teacher.

Virus Checks

All computers in school have anti-virus software, although very new viruses will not be found. If you suspect a virus, please report it to the ICT technician straight away.

Legal Requirement

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please discuss this with the ICT technician or Computing Leader. Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head Teacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random-access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at any time. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

12. Sanctions

If children break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

13. Children with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each child. Where a child has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Allegations against Adults Who Work With Children and Young People
Allegations made against a member of staff should be reported to the Senior Designated Officer for safeguarding within the school immediately. In the event of an allegation being made against the Executive Head Teacher, the Chair of Governors should be notified immediately.

14. Local Authority Designated Officer (LADO) - Managing Allegations

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

15. Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Additional Information
Please be aware, at such time that you leave Manston Primary School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

If children, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Head Teacher for further guidance. This agreement applies to all online use and to anything that may be downloaded or printed.

16. Appendices

- Appendix 1 - Pupil AUP
- Appendix 2 - Staff AUP
- Appendix 3 - Governor AUP

Appendix 1

Pupil Acceptable Use of Internet and Digital Technologies Policy Staff Agreement

Pupils Acceptable Use Agreement

Respectful Communication:	•Use only respectful language online and avoid sending negative messages.
Personal Information:	•Keep all personal information private and never share passwords.
Careful Clicking:	•Always be careful when clicking on links or downloading files and check with an adult first.
Educational Use:	•School accounts, emails, TTRS, and other digital tools and equipment are strictly for educational purposes and will only be used by the assigned pupil. Follow the rules set by your teachers.
Reporting Issues:	•If something online makes you feel uncomfortable, immediately tell an adult.
Digital Responsibility:	•Your online actions are permanent, so act in a way that you can be proud of.
No Cyberbullying	•Cyberbullying is unacceptable. Report it if you experience or see it.
Image Sharing:	•Get permission before posting or sharing images and videos.
Positive Online Presence:	•Act responsibly online and be a positive influence.
Monitoring:	•The school monitors technology use to ensure safety and compliance.
Sanctions for Misuse:	•Misusing technology may lead to consequences, including discussing the issue at home, and in serious cases, informing future schools.

Manston

Staff Acceptable Use of Internet and Digital Technologies Policy Staff Agreement

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. Staff agree to this Acceptable Use Agreement so that they provide an example to children and young people for the

safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

All staff agree to the following

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to obtain permission for children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people. (pupils names shown in pictures)
- I have read the procedures or incidents of misuse in the Internet and Digital Technology Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person in accordance with procedures listed in the Acceptable Use Policy.
- I know who the Designated Safeguarding Officers are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail.
- I know I should use the school e-mail address and phones to contact parents and other members of staff.
- I know to copy in the Head Teacher into any email to a pupil and for any emails to parents that they need to be made aware of.
- I know that I must not use the school system for personal use unless this has been agreed by the Head Teacher.
- I know that I should notify the school ICT lead/technician to perform a virus check on my laptop and other storage devices that I wish to use so that I do not inadvertently transfer viruses especially where I have downloaded resources. If I am unsure, I must not do anything and notify the ICT lead/Datacable immediately.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Head Teacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden.
- I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been shown a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

Acceptable Use of Internet and Digital Technologies Policy

Children and parents agree that

- Users are responsible for good behaviour and following the school values on the Internet just as they are on school premises. General school rules apply.
- The Internet is used within school to conduct research, access educational material and communicate with others.
- The permission of parents/carers is required for pupil use of school devices outside of school. Parents/carers are responsible for any loaned devices and must immediately inform school or any issues or problems.
- Staff may review files and communications to ensure that users are accessing the system responsibly.
- Users should not expect that files stored on school equipment, servers or the school network would always be private.
- During school, teachers will guide children towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, movies, radio and other potentially offensive media.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using other users' passwords or passing password information onto others
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use in school and use of any school managed programmes outside of school.

2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

For Staff: By reading this document, and 'marking as read' on CPOMS, I am agreeing to understanding and implementing all of the contents within this policy and recognise that there will be sanctions should I violate any of these statements.

Appendix 3

Governor Acceptable Use of Internet and Digital Technologies Policy Agreement

Governors have a duty to ensure that the school and its staff, including themselves, are aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. All governors must agree to this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

1. I understand that ‘digital’ includes networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, smart watches, digital cameras, email and social media sites**.**
2. School owned information systems including TEAMS, must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by Manston Primary School can only be used by members of staff and governors and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware or to add anyone from outside of the school community to the school TEAMs account without permission from the system manager.
6. I will ensure that any school data or reports (that mention or contain information about or could identify pupils, staff or parents/carers) are kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
7. I will not keep or access documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted.
8. I will not store any personal information on the school system that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will respect copyright and intellectual property rights.
10. I will report all incidents of concern regarding digital safety to the Designated Safeguarding Lead (James Clay), his deputy (Kirsty Thorpe) and/or the ICT Manager (Karen Cartwright) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to James Clay and or Kirsty Thorpe in his absence.
11. I will not attempt to bypass any filtering and/or security systems put in place by the school.
12. My electronic communications with staff, parents/carers will take place within clear and explicit boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels- TEAMS, phone call from school office and not via personal devices or communication channels e.g. social networking or mobile phones.
13. I will ensure that my online reputation and my use of digital and information systems are compatible with my role.
14. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
15. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the ICT Manager or the Head Teacher.
16. I understand that my use of the information systems, Internet and email on school systems may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Governor Acceptable Use Policy.

Signed: …….. Print Name: …… Date: ……

Accepted by: …… Print Name: ……