Marshfield Primary

ICT Policy

Policy history: Updated	**Date: November 2022**
Written	**June 15th, 2019**
Agreed by Full Governors	**December 2022**

Marshfield Primary School – Internet Access Policy

Contents

The Importance of Accessing the Internet in School

The purpose of using the internet in school is to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Both staff and pupils have access to the internet, and we believe it is an essential life skill for the 21st century.

Staff and Pupils benefit from accessing educational resources from around the world, from museums to libraries, to universities and art galleries, and an array of commercial resources. They also have access via the Welsh Government HWB learning platform, and the array of resources that it offers.

Assessment of Potential Risk

The international and linked nature of information accessible on the internet means that it is not possible to guarantee that certain types of material will not appear on screen.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Marshfield Primary School cannot accept liability for all material accessed, or any consequences thereof. The school will, however, provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks including a robust filtering systems to prevent certain types of information being accessed.

As a School we believe that equipping children and adults with a robust online safety ethos is an essential element of safeguarding when using the array of technology available, including computers, tablets, mobile phones or games consoles whether at home or in school. This policy aims to provide a framework to achieve this.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school as well as children and parents/carers.

This policy must be read in conjunction with other relevant school policies including safeguarding and child protection, anti-bullying, behaviour, data security, and Acceptable Use Policies.

The Headteacher and the SLT will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

Before access is granted

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Staff Acceptable Use Policy and the Pupil Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Responsibilties of those Accessing the Internet in the classroom

Staff

- Ensuring that they have an up to date awareness of e-safety matters
- Reading and adhering to the school's e-safety policy and practices
- Reading, understanding and signing the school Staff Acceptable Use Policy
- Reporting any suspected misuse or problem to the Headteacher
- Ensuring any digital communications with pupils are on a professional level and only carried out using official school systems
- Ensuring that E-safety issues are embedded in all aspects of the curriculum and other school activities
- Ensuring that pupils understand and follow the school e-safety and acceptable use policy
- Monitoring ICT activity in lessons and extended school activities
- Teaching children so that they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Ensuring pupils are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices
- Using suitable internet sites during planned lessons, staff will carefully check sites for content prior to including in lessons.
- Ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- There is an awareness that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Should any sites appear unsuitable, the URL must be noted and immediately reported to the School Business Manager or ICT Co ordinator.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- They should know and understand school policies on the taking/use of images and on cyber-bullying
- They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Reporting immediately any unsuitable sites to their class teacher or responsible adult in the class.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided, which will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

- Pupils should be helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- All staff should act as good role models in their use of ICT, the internet and mobile devices

Parents

Marshfield Primary School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

- Parents' attention will be drawn to the school ICT policy and expectations in newsletters, letters, and the Parent Acceptable Use Policy.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Community Users

- Community Users who access school ICT systems as part of the extended school provision will be expected to sign a Community User AUP before being provided with access to school systems.

Communication Mediums

Email

- Pupils need to use email as part of our ICT scheme of work.
- Pupils may only use school provided email accounts for educational purposes
- Pupils are given individual email addresses to be used via the HWB.
- All members of staff are provided with a specific school email address to use for any official communication.

- Pupils will use email during planned lessons, but will be informed by their teacher that content will be checked periodically for appropriateness.
- Forwarding chain emails is not permitted.
- Class teacher must be informed immediately of any inappropriate email content.

Social Media

General social media use

Expectations regarding safe and responsible use of social media will apply to all members of Marshfield Primary and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include Twitter, the school website and applications such as Seesaw, PFA Facebook page.

- All members of our school will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of staff at and pupils at Marshfield Primary School.
- All members of our school are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the Photo Consent Form signed by parents.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems i.e. Twitter
- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Marshfield Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.

Pupil's use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.
-

School website

- The school will ensure that information posted on the school website will comply with the schools guidelines for publication.
- The contact details on the website will be the schools address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- All material must be the authors own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- Pupils work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.
- The ICT team in consultation with the head teacher shall provide limited editorial access for other members of staff.
- The school shall not be responsible for the content of any website to which websites provide a link, although such websites as Children's BBC are checked before adding. As they are beyond the control of the school, it is possible that the page could alter after it has been deemed acceptable in school.
- Group photographs should not have name lists attached.
- Permission from parents/carers will be sort through our 'Letter of photo consent' to publish photographs of the children on the school website/Twitter or for promotional material including the Annual School Calendar of Events as well as being used in press/media photographs or videos. It is the parental responsibility of parents and carers to contact the school if they wish to withdraw consent at any time
- A record shall be kept by each class of these children who do not have permission for photographs to be published.

Official video conferencing and webcam use for educational purposes

- As part of our ICT Scheme of work Pupils will be able to access webcam and videoconferencing programs via the HWB.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.
- Pupils will access videoconferencing via the HWB

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

HWB

- Leaders/managers and staff will regularly monitor the usage of the HWB in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the HWB.
- Only members of the current pupil, parent/carers and staff community will have access to the HWB.
- All users will be mindful of copyright issues and will only upload appropriate content onto the HWB.

Any concerns about content on the HWB will be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the HWB for the user may be suspended.

d) The user will need to discuss the issues with a member of leadership before reinstatement.

e) A pupil's parent/carer may be informed.

Personal Devices and Mobile Phones

- Children are not permitted to use mobile phones, including smart watches on the school premises.
- Parents/Carers and Visitors are not permitted to use their mobile phones on school premises for photographic purposes. NB. The school's leadership team may give permission for these in certain circumstances.
- Parents/carers and visitors must not publish video or photos of any other child/staff member on any social media platform without their express permission
- Staff will not use mobile phones within the classroom.
- Contractors will only take photographs of a building related to the job that they are working on. They must be supervised in this action by a member of staff, who will check and ensure no child is within the shot. Beyond this, no contractor must take photos.
- **Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors**

Training for Staff

Information Security

All staff handle sensitive data, both hard copy and digital, on a daily basis. It is each person's responsibility to ensure that data is secure and not accessible to malicious third-party access. Training will take place on induction of new staff and at formal staff meetings throughout the year.

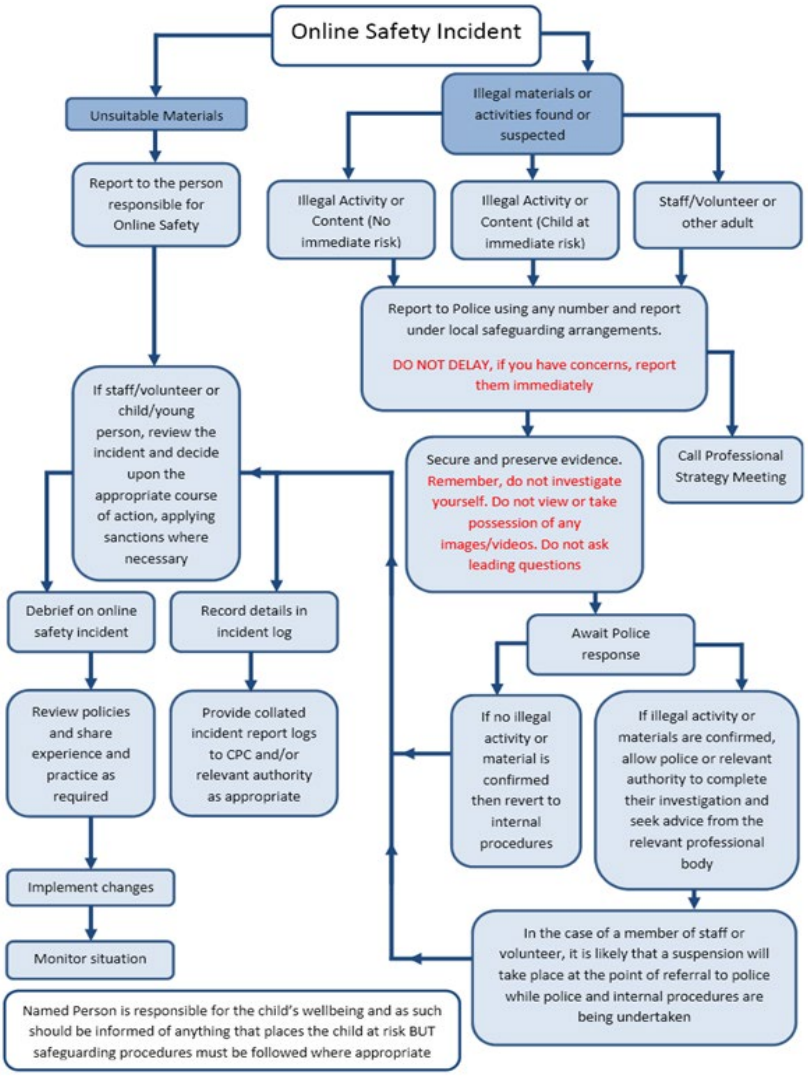
Cyber Security

Cyber security is about protecting the devices we all use and the services we access online from theft and damage. All staff to undertake the National Cyber Security online training on induction or throughout the school year.

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If there is any suspicion that a website(s) contain suspected illegal activity, refer to the right hand side of the flowchart below for responding to online safety incidents and report immediately to the police.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures as follows:

APPENDIX 1 – Overview of User Permissions

	Staff				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other personal camera devices				✓				✓
Use of hand held devices e.g. i pads	✓				✓			
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓

Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs	✓						✓	

APPENDIX 2 - - Sanctions for Misuse - Staff

Incidents:	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for Action re filtering	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal				✓				✓
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email during school time		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓						
Careless use of personal data, e.g., holding or transferring data in an insecure manner		✓						

Deliberate actions to breach data protection or network security rules		✓				✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓		✓		✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓						
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with pupil		✓				✓		
Actions which could compromise the staff member's professional standing	✓	✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓						
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓			
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		

Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				✓
Breaching copyright or licensing regulations		✓						
Continued infringements of the above, following previous warnings or sanctions								✓

Appendix 3 – Sanctions for Misuse - Pupil

Incidents:	Refer to Class Teacher	Refer to LAST	Refer to Headteacher	Refer to Police	Refer to technical support for action	Inform parents/carers	Removal of network access rights	Warning	Further sanction, e.g., exclusion
Deliberately accessing or trying to access material that could be considered illegal			✓	✓		✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone/digital camera/other handheld device	✓								
Unauthorised use of social networking/instant messaging/personal email		✓	✓						
Unauthorised downloading or uploading of files	✓								
Allowing others to access school network by sharing username and passwords	✓								

Attempting to access or accessing the school network, using the account of a member of staff		✓	✓						
Corrupting or destroying the data of other users		✓	✓						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions									✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓				
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓				
Deliberately accessing or trying to access offensive or pornographic material				✓		✓	✓	✓	✓

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓						

Appendix 4 – Parent/Carer Acceptable Use Agreement

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies including Social Media are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Social Networking
Concerns have been raised over some of the possible issues including:

- Interaction between teachers and pupils or parents.
- Inappropriate communications between colleagues.
- Unpleasant or abusive postings about teachers or pupils.
- Criticism of the school (not personally abusive).
- The setting up of fake profiles

Any form of misuse directed at the school, its employees, the pupils or anyone associated with the school will be taken very seriously. If any illegal activity or content is suspected the school will inform the necessary authorities.

The school wishes to remind its parents that Facebook and other Social Medias are only intended for users aged over 13. The school also understands that it is very easy for young people (or indeed adults) to enter an incorrect date of birth or false information to open an account. In fact, according to Ofcom's UK Media Literacy report (April 2011) "social networking continues to increase and 47% of 10 – 12 year olds have an active profile".

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Thank you for your cooperation

Lisa Lewis
Head Teacher

PARENT/CARER ACCEPTABLE USE AGREEMENT

(Please read, sign and return to school)

Parent / Carers Name:…….

Student / Pupil Name:……

1. As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

2. I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

3. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

4. I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

5. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

6. I agree that my child will not bring a mobile phone to school, or on a school trip (particularly residential visits) as I understand that this presents a safeguarding issue when photos and videos can be taken of other children.

Signed:…….

Date:……

Appendix 5 FP Pupil Acceptable Use

Marshfield Primary School Acceptable Use Agreement

Foundation Phase

This is how we stay safe when we use computers:

- ☺ I will ask a teacher or another adult from the school if I want to use the computers;
- ☺ I will only use activities that a teacher or another adult from the school has told or allowed me to use;
- ☺ I will only use websites that my teacher has agreed to let me use;
- ☺ I will take care of the computer and other equipment;
- ☺ I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong;
- ☺ Email only - I will only use my hwb office365 email and google mail on the school premises and not at home;
- ☺ I will only access my hwb email and not my private email whilst in school;
- ☺ I will not use email during lessons, unless the teacher has permitted its use;
- ☺ If I receive an email from a person I do not know or one that upsets me, I will immediately show it to the class teacher;
- ☺ Do not open anything from anyone you do not know;
- ☺ I will tell a teacher or another adult from the school if I see something that upsets me on the screen.
- ☺ I will not arrange a meeting with anyone met via web or email without the permission of my parent/carer.

- ☺ I know that if I break the rules I may not be allowed to use a computer/tablet.

Appendix 6 – KS2 Acceptable Use

Marshfield Primary School Acceptable Use Agreement

Years 3-6

This is how we stay safe when we use computers:

- ☺ I will ask my teacher/parent/carer if I want to use the computers;
- ☺ I will take care of the computer and other equipment;
- ☺ I will immediately report any damage or faults involving equipment or software, however this may have happened to my teacher/parent/carer;
- ☺ I will only use activities that a teacher or my parent/carer has allowed me to use;
- ☺ I understand that Hwb, Office 365, emails and the TEAMS platform are only for educational use;
- ☺ I will search the internet on teacher directed sites only, and will not randomly search other topics.
- ☺ Email only - I will only use my hwb office365 email and google mail on the school premises and not at home;
- ☺ I will only access my hwb email and not my private email whilst in school;
- ☺ I will not use email during lessons, unless the teacher has permitted its use;
- ☺ I will be polite and responsible when I communicate with others;
- ☺ Do not open attachments from senders you do not recognise or that look suspicious;
- ☺ I will not forward on any emails to other pupils unless requested to by my teacher;
- ☺ If I receive an email from an unknown person or one that is offensive or upsetting, I will immediately show it to the class teacher.
- ☺ I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, etc.)
- ☺ I will respect others' work and will only access, copy, remove or alter anyone else's files, with their knowledge and permission;
- ☺ I will ask for help from a teacher or another adult in school or at home if I am not sure what to do or if I think I have done something wrong;
- ☺ I will tell a teacher or another adult from school or at home if I see something that upsets me on the screen;
- ☺ I will not arrange a meeting with anyone met via web or email without the permission of my parent/carer;
- ☺ I will not bring a mobile phone on site or on school trips (either day or residential trips).

- ☺ I know that if I break this agreement in anyway there will be consequences for my actions.

Signed:

Appendix 7 Marshfield Primary Staff ICT Acceptable Use Policy

The computer system is owned by the school and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's Staff ICT Acceptable Use Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

All staff (including supply and temporary) requiring Internet access should sign a copy of this Acceptable Use Statement and return it to the School Business Manager for approval.

Users must also accept personal responsibility for reporting any misuse of the network to Mr Mrs C Dixon (Marshfield Primary School) and Mr T David (Newport High School.

Conditions of Use

It is the personal responsibility of every user to take all reasonable steps to make sure they follow the conditions set out in this Policy.

Professional Standards and the Network

1. I understand that the school will monitor my use of the school digital technology and communications systems.
2. I understand that the rules set out in this agreement apply to the use of all technologies available to me (e.g. desktops, laptops, ipads, email, HWB etc.) both in and out of school, and to the transfer of personal data (digital or paper based) out of school.
3. I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
4. I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school (or Newport City Council) into disrepute.
5. I will use appropriate language - I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
6. I will not use language that could stir up hatred against any ethnic, religious or other minority group.
7. I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
8. I will not trespass into other users' files or folders.
9. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
10. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Mrs C Dixon or Mr T David.
11. I will ensure that I log off after my network session has finished.
12. If I find an unattended machine logged on under other users username I will not continuing using the machine - I will log it off immediately.
13. I understand that I am not allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
14. I will ensure that my data is regularly backed up to the cloud via either my H:drive, N:driver, T: drive

or U:drive

15. Anything that needs to be shared will be shared through the staff shared area or T: drive or One Drive.
16. I will not save data on my desktop as I risk losing the data
17. I will not use the network in any way that would disrupt use of the network by others.
18. I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to Mrs C Dixon or Mr T David.
19. I will not introduce "USB drives" or other portable devices into the network without having them checked for viruses.
20. I will lock my PC/laptop if temporarily leaving it unattended.
21. I will not allow pupils to use a PC/laptop that is logged in with my username and password. I will always ensure pupils connect using their appropriate credentials.

Email, Website and Social Media Access

1. I am aware that e-mail is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted.
2. I will not use personal email addresses to correspond on school matters, or use my school email address for private matters.
3. I will always check that recipients of email messages are correct before sending.
4. **I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)**
5. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
6. I will not download and/or install any unapproved software, system utilities or resources from the Internet.
7. I will not become "friends" with children on any social networking sites or engage with children on internet chat.
8. I realise that users under reasonable suspicion of misuse in terms of time, activity or content may have their usage closely monitored or have their past use investigated.
9. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
10. I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
11. I agree to comply with the acceptable use policy of any other networks that I access
12. I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
13. I will only use school registered email addresses to manage official social media accounts e.g. Twitter, SeeSaw.
14. I will not use my personal equipment to record these images e.g. on a mobile phone, unless I have permission to do so. Where these images are published (eg on the school website / Twitter) it will not be possible to identify by name, or other personal information, those who are featured. access.
15. I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
16. I will not engage in any on-line activity that may compromise my professional responsibilities. The school and the local authority have the responsibility
17. I will only use social networking sites in school in accordance with the school's ICT Policy.
18. I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

19. I will not add any pupil or pupil family member as a 'friend' on any social networking site.
20. I will advise the Headteacher if a pupil or pupil family member is attempting to contact me via any social media platform outside of school.
21. I will not engage in any on-line activity that may compromise my professional standing.
22. I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
23. Where work is protected by copyright, I will not download or distribute copies (including music and videos). I understand that I am responsible for my actions in and out of the school.
24. I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
25. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

Data Protection

1. I understand that if I need to make use of personal data, sensitive or confidential information outside of school environment, I will put in place sufficient safeguards to mitigate the risks of loss or misuse.
2. I will only use One Drive to transfer/upload files.
3. I will only use an encrypted pen drive for sensitive data.
4. I will ensure that all data relating to staff, students and parents will be kept private and confidential.
5. I will ensure that sensitive information will be securely disposed of.
6. I will protect any sensitive material to the same level as paper copies including using Secure Print option when materials are being printed or shared.
7. I will immediately report any loss or theft of equipment, and will ensure that laptops taken off site are not left in any vehicles.

I have read and accept the Acceptable Use Policy (Pages 1-3) in its entirety.

Name: _____

Position: _____

Date: _____

Appendix 8 Live Streaming Acceptable Use Agreement

There are a number of key considerations to ensure safe and effective use of live-streaming that parents/children need to follow. These include:

1. Location
    a. choose a neutral location that is appropriate and safe e.g. living room, study or kitchen NOT A CHILD'S BEDROOM.
    b. It would be preferable to have child accompanied, or within easy access of a parent/carer.
    c. Ensure there are no distractions or interruptions from other household members or pets.

2. Equipment and Camera Settings
    a. Ensure that laptops and chargers are plugged in and ready for the session
    b. Carefully consider what is in view of the camera i.e. check the background is professional and does not contain images or information that should not be shared or deemed inappropriate.

3. Behaviour
    a. Children must log in promptly to the lesson
    b. Children should dress appropriately, as if coming in to school on a non-uniform day e.g. no pyjamas
    c. All microphones must be muted at the start of the lesson
    d. Children must raise their online hand if they wish to speak and must not shout over other participants
    e. "Classroom Standard" behaviour is expected from all children

4. Privacy and GDPR
    a. Children/adults are strictly forbidden to take or share images of the lesson
    b. Children/adults are strictly forbidden to record the lesson

5. Safeguarding
    a. Children will be admitted to the "class" by the teacher
    b. The teacher will ensure that every child is logged out of the lesson, and that no children are left unsupervised

Updates:

Review/Ammend Date:	Reason:
March 2020	Appendix 8 – Use of TEAMS by children for remote learning required additional securities. Shared to parents and children.
Nov 2022	Appendix 5 – Foundation Phase Pupil Acceptable use – Email specific use inserted
	Appendix 6 – KS2 Pupil Acceptable use – Email specific use inserted
	Appendix 7 - New points in Staff Acceptable Use section highlighted in yellow
January 2023	Training – Information Security and Cyber Security Training added