WEXHAM COURT PRIMARY SCHOOL

E-Safety Policy

2021 - 2024

Date Approved:	**Autumn 2021**
Date for Review:	**Autumn 2022**
Approved By:	**Head Teacher & Full Governing Board**

WEXHAM COURT PRIMARY SCHOOL

E-SAFETY POLICY

Preparing every child to become a successful individual in an ever evolving world.

Build belonging, Strive for excellence and Do the right thing.

At Wexham Court Primary School we are proud of the diversity of our students and staff and are committed to promoting a positive and inclusive culture in which all are valued and supported to fulfil their potential irrespective of their age, disability, race, religion, beliefs, sex or sexual orientation. We acknowledge that we are all influenced by implicit bias, or the stereotypes that unconsciously affect our decisions and that this can negatively impact traditionally marginalised and disenfranchised students. In all areas of our school, we strive to understand and appreciate all aspects of diversity, equality and inclusion and proactively adapt our school policies and procedures accordingly.

1. Rationale

Today's pupils are growing up in a world where online and offline life is almost seamless. This offers many opportunities but also creates challenges, risks and threats. At Wexham Court Primary school we try to equip our pupils with the knowledge to be able to use technology to their best advantage in a safe, considered and respectful way.

Our vision acknowledges an ever-evolving world, therefore at Wexham Court we embrace technologies whilst remaining every vigilant about the associated risks. Our values underpin our approach.

- Build belonging- we are able to connect to a community beyond our school and network with people that we know and trust.
- Do the right thing – children are taught to reflect on their choices and make a decision that is right for all. Children are to apply their knowledge of internet safety to ensuring they make positive choices for all whist online
- Strive for excellence - to embrace new technology and grow alongside it, equip children with the skills and knowledge they need.

Wexham Court is a Microsoft showcase school, through which we develop staff knowledge and skills around IT and how it can effectively enhance the curriculum

Our school community recognises the importance of treating e-safety as an ever-present serious safeguarding issue and its teaching as a whole school issue and the responsibility of all staff. It is important to protect and educate both pupils and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Ofsted reviews e-safety measures in schools and there are numerous Acts of Parliament which relate when considering the safeguarding of both staff and pupils in schools. The safeguarding aspects of e-safety are evident in all our IT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review.

It is also critical to ensure the safety and security of all personal data that the school holds and processes. Under the General Data Protection Regulation, the school is responsible for exacting standards of safety and security of personal data that may be processed.

This policy should be read in conjunction with our Safeguarding and Child Protection, Social Media, Remote Learning and Behaviour policies. This policy links all the IT, safeguarding and other policies and procedures to reflect how the school deals with e-safety issues on a daily basis.

In this policy 'Staff' refers to all adults, as we recognise that all adults have a shared duty of care to our pupils.

2. The Technologies

Information Technology (IT) in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of IT creating a safe IT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;

2. Policies and procedures, with clear roles and responsibilities;

3. A comprehensive E-Safety education programme for pupils, staff and parents.

3. Staff Responsibilities

3.1 All Staff

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. An audit of the e-safety training needs of all staff will be carried out regularly. Training will be offered as a planned programme of formal e-safety training available to all staff. All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

Staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy.
- They have read, understood and signed the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies eg staff e-mail, social media, use of personally owned IT devices and professional identity protection.
- They report any suspected misuse or problem to the e-safety co-ordinator/Head Teacher/senior leader/head of IT/class teacher/head of year as appropriate for investigation/action/sanction.
- They report any suspected breach of processing any personal data to the e-safety co-ordinator/headteacher/senior leader/ network manager/technical support provider.
- Digital communications with pupils (email/virtual learning environment (VLE)/voice) are on a professional level and only carried out using official school systems.
- Pupils understand and follow the school e-safety policy and the pupil acceptable computer usage policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor IT activity in lessons and in extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

- They are aware of the e-safety issues pertaining to email and social media usage.
- They are alert to, and report to the headteacher, any suspicions of pupils who may be becoming radicalised.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.2 Designated Safeguarding Lead (DSL)

The DSL is trained in e-safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Peer on Peer Cyber-bullying.
- Sexting.
- Suspicions of radicalisation.

4. Internet:

1. Wexham Court Primary School use a filtered Internet Service, which minimises the chances of pupils encountering undesirable material.
2. Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.
3. Staff should email school-related information using their Microsoft 365 address and not personal accounts.
4. Staff will preview any websites before recommending to pupils.
5. Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/.
6. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
7. E-Safety information is found on the school website as well as links to CEOPs website.

8. If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the E-Safety coordinator(s) detailing the device and username. The filter can then be investigated and improved further.

9. Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.

10. Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a staff member who will report it to the Computing-Co-ordinator so that the Service Provider can block further access to the site. The computing lead should keep a record of any reports and share with the DSL.

11. Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.

12. They are taught the rules of etiquette in email and are expected to follow them.

13. No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

14. Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.

15. A summary of these IT rules (SMART RULES) are displayed in the IT suite and all areas with IT resources. Pupils will be asked to sign to this agreement, ensuring that they are aware of expectations. (See Appendix). Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

5. Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.
- Passwords should never be auto filled.

6. Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.

Please refer to the laptop loan agreement that all staff are required to sign for more information.

- Mobile technology for pupil use, such as iPads, visualisers are stored in a locked Safe. Access to the laptops is available via the school office keyholders. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.

- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.

- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

- No personal devices belonging to staff or children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent and out of sight of children.

7. Data storage:

- Staff are expected to save all data relating to their work to the school Sharepoint and <u>not</u> in personal documents.

- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.

- SEN plans, assessment records, photographs, pupil medical information and any other data related to pupils or staff should not be stored on personal memory devices

- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure, speak to a member of the Senior Leadership Team.

8. Social Networking Sites (see Social Media Policy for more information):

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.

    - Ensure all social media profiles are secure and on private settings

    - Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.

    - Your role in school requires a high degree of professionalism and confidentiality.

- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.

- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use. Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - or using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

If you become aware of peer on peer cyberbullying through social media platforms, please refer to the Behaviour Policy for the procedures to deal with this. **The School reserves the right to monitor staff internet usage. The School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.**

9. Digital images:

When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- If any incidents come to light about 'sexting' i.e. the sharing of sexual images of pupils under 18, the Head Teacher and DSL should be advised in the first instance.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.

- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Ensure you are aware of children whose parents/guardians have not given permission for their child's image to be used in school. An up to date list is kept in the school administrative office, with the Head Teacher and Senior Leaders and the Head Teacher's PA.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

10. Providing a comprehensive E-Safety education to pupils and parents:

- All staff working with children must share a collective responsibility to provide E-Safety education to pupils and to promote E-Safety in their own actions.
- Formally, an E-Safety education is provided by the objectives contained in the IT unit plans for every area of work for each year group. Even if E-Safety is not relevant to the area of IT being taught, it is important to have this as a 'constant' in the Computing curriculum. It is also formally taught through PSHE and specifically in Health and Relationships Education.
- Informally, a talking culture is encouraged in classrooms which allows E-Safety issues to be addressed as and when they arise.
- The Computing Coordinator will lead an assembly twice a year, including on Safer Internet Day, highlighting relevant E-Safety issues and promoting safe use of technologies.
- All classes will follow a themed week at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.
- In Years 5 and 6 E-safety will be taught with more prevalence, through programmes such as the Choices project
- Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the computing Coordinator with responsibility for E-Safety.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines. (See Appendix)
- Parents/carers will be invited to attend an E-Safety awareness workshop once per year, run by the Computing Co-ordinator and DSL.

11. E-safety in the curriculum

E-safety is taught in specific areas of the curriculum but is also emphasised whenever pupils are using computers online. Staff always consider age-appropriateness when speaking of e-safety and will be aware of those pupils who may be particularly vulnerable, e.g. looked-after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them.

All children at Wexham are taught to view E-Safety through the lense of our school behaviour code "being ready, respectful and safe", for example being as respectful to people online as you would be in person and that we are not 'keyboard warriors'. When we teach the children about online safety we emphasise that technology is a positive part of education and the world around them and advocate for the children to keep themselves and others safe online.

11.1 Health and Relationships education

Pupils are taught about:

- Online safety and harm.
- Positive, healthy and respectful relationships online.
- The effects of their online actions.
- How to recognise and show respectful behaviour online.
- How to look after their mental health
- What content online is age appropriate and how long should be spent online

11.2 Computing in the curriculum

- Principles of online safety.
- Where to obtain help and support if they are concerned about any online content or contact.

11.3 E-safety throughout the curriculum

Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities, including:

- How to evaluate what they see online – to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- How to recognise persuasion techniques.
- How to recognise acceptable and unacceptable online behaviour – to understand the need for the acceptable computer usage agreement and to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- How to identify online risks.
- How and when to seek support.
- The need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.

It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.

12. Maintaining the security of the school IT Network:

Tri-Computers maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network.

The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the acceptable computer usage policy and any relevant LA e-safety policy and guidance.
- Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- There will be regular reviews and audits of the safety and security of school IT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the Tri-Computers.
- All users will be provided with a username and password by Tri-Computers.
- The 'master/administrator' passwords for the school IT system including the Wifi password, used by Tri-Computers are also available to the Head Teacher or other nominated persons and kept in a secure place (e.g. school safe).
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed filtering service provided by Tri Computers.
- Any filtering issues should be reported immediately to Tri-Computers.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.
- Agreements are signed by members of staff in possession of school-provided laptops regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other personally owned devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date virus software.

13. Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation of pupils.

Should any serious e-safety incidents take place, the appropriate external authorities will be informed e.g. local area DSL, police etc or, for personal data breaches, the Information Commissioner's Office (ICO).

Members of staff who are found to be producing covert recordings, whether audio or visual, on any form of electronic device, whether owned by the school, or a personal device, will face disciplinary action.

14. Complaints procedure:

Complaints will follow the school's complaints procedure and policy.

15. Monitoring:

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any IT equipment owned or leased by the school at any time without prior notice. Monitoring includes: intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School IT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

16. Breaches of Policy:

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings. Incident Report All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's Designated Safeguarding Officers or head teacher.

This is a true version signed by

Mr J. Reekie, Chair of Governors

Signed: Date:

Miss N Mehat Headteacher

Signed: Date:

Review date: Autumn 2024

Appendix 1 Useful organisations/support services for reporting e-safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at https://iwf.org.uk

Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

Online content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.

Getting help/advice: for parents and carers

- Advice from the DfE on keeping children safe online during remote learning can be found at: www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online.

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk

- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 5pm, Mondays and Tuesdays on 0207 823 5430 www.kidscape.org.uk.

- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'. Contact details are: www.childnet.com phone 020 7639 6967, email info@childnet.com.

- *UK council for internet safety (UKCIS)* has practical guides to help parents and others with internet safety www.gov.uk/government/organisations/uk-council-for-internet-safety.

- *Thinkuknow* has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

Getting help/advice: for teachers

DfE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gov.uk) to enable teachers to raise concerns or questions on extremism directly with them.

Appendix 2 - Wexham Court Primary School

IT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from E-Safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will password protect all school devices or systems.
- I will not disclose my password to anybody else, or use search engines to save any to file.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- I will report any E-Safety concerns to the designated safeguarding officer immediately using the Incident Log Form.
- Mobile phones will be out of sight and switched to silent.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's E-Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.

- When using TEAMs or other technology to teach, I will adhere to the terms stipulated by the Head Teacher, the Social Media Policy and the Remote Learning Guidance.

I understand the procedures and agree to follow them with immediate effect.

Print Name: _____ Signed: _____

Date: _____

Appendix 3 - Wexham Court Primary School

Pupil Acceptable Use

The school has provided computers and tablets with internet access to help your learning. You have also been provided with a Microsoft Teams account. These rules will keep us safe and help us to be fair to others.

- I will only use school ICT equipment for learning purposes.• I will ask permission from a member of staff before using the internet and will only go online when an adult is in the room.
- I will only use my own login and password and never share these with others.
- I will only use Teams, whether at school or at home, to support my learning.
- I will only message my teachers on Teams, or other staff who work at the school, during school hours to support my learning.
- I will not use Teams in or out of school to message my friends or speak to other adults who do not work at the school.
- I will inform my teacher immediately if my friends or an adult who does not work at the school tries to speak to me on Teams.
- I will only open, edit and delete my own files.
- I will not download or delete any apps on the computers, laptops or iPads unless I have been given permission to do so by an adult.
- I will ensure I use the technologies carefully, never removing the iPads from the case or run with one.
- The messages I send will be polite and sensible.
- I will never give out my own or other people's name, address or phone number online.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.

- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away.

- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my E-Safety.

Pupil Signed: _____ Date:_____

Class: _____

Wexham Court Primary School – Laptop Loan Policy

Church Lane, Wexham,
Slough, Berkshire
SL3 6LU
Telephone: 01753 524533
Fax: 01753 512029
Email: mail@wexhamcourt.slough.sch.uk
www.wexhamprimary.com

Head Teacher:
Miss N Mehat BA, QTS, N.P.Q.H

Part of Wexham Court Primary School's Improvement plan is to provide laptops to staff to assist in the delivery of the National Curriculum. Following consultations on the allocation of computers under the DfE laptops for Teachers initiative, it has been recommended that a laptop be loaned to you while you remain employed at the school. While the laptop is in your care, you must abide by the following;

1. The laptop and peripherals it is issued with remains the property of Wexham Court Primary School and is only for the use of member of staff it is issued to.

2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft from an unattended car. If the laptop is stolen from an unattended car, you will be responsible for its replacement. The cost of the laptop will be the full cost of the laptop in Year 1 and half the cost of the laptop in Year 2.

3. Only software licensed by the school and approved by IT Support and the Head teacher are installed. Any other software that is required must be authorised. Any pirated or unlicensed software that is installed will result in action taken against that member of staff it has been assigned to.

4. It is your responsibility to bring in the laptop on a weekly basis and connect it to the schools network so that it can receive updates from the schools server. Not doing so will

result in login issues and leaving the laptop vulnerable from external threats such as viruses.

5. Any internet charges incurred by staff accessing the internet from home whilst using the laptop are not chargeable to the school.

6. Any internet content that is accessed whilst connected to the schools network is monitored through a proxy server. Social networking, chat rooms and adult content are some of the categories that are strictly prohibited in a work environment as well as protecting the safety of the children during ICT lessons. If any of these restricted categories are accessed offsite the member of staff will be held responsible and if found guilty, appropriate action will be taken.

7. Should any faults occur with the laptop or its peripherals, IT support must be informed as soon as possible to ensure that they can undertake any necessary repairs. Under no circumstances should the staff attempt to fix any suspected faults with the laptop or its peripherals.

8. If any member of staff needs help in operating either the hardware or software that comes with the laptop then please contact IT support. Training can be provided to ensure that teaching whilst using the laptop doesn't get affected.

9. The schools policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by the users of the laptop.

Please read the above carefully and sign below:

Failure to take reasonable care or abide by the conditions listed in this document may result in the Laptop being reclaimed.

I have read, understand and agree to abide by the terms of the Wexham Court Primary School **Laptop Loan Policy.**

Signature:

……

Please Print Name:

……

Date:

Church Lane, Wexham,
Slough, Berkshire
SL3 6LU
Telephone: 01753 524533
Fax: 01753 512029
Email: mail@wexhamcourt.slough.sch.uk
www.wexhamprimary.com

Head Teacher:
Miss N Mehat BA, QTS, N.P.Q.H

User Responsibilities

- The iPad screen is made of delicate glass, therefore it can be subject to cracking and breaking if misused; never drop or place heavy objects (books, laptops etc) on the iPad.
- The iPad has a case for its own protection, it should not be taken out of it nor should it be covered in stickers or unnecessary sticky notes.
- A microfiber cloth and approved laptop cleaning fluid should be used to clean the iPad.
- Do not subject the iPad to extremes of temperature as it can cause irreparable damage.
- The whereabouts of the iPad must be known at all times.
- It is the user's responsibility to keep the iPad as safe and secure as possible when not in use by applying a passcode and locking it away using the safe's provided in the classroom.

Safeguarding

- Users may not take photos of any other person without that persons consent.
- Photographs of children must be in line with the schools safeguarding policy.
- Images of other people may only be made with the permission of the person, or the parents of the person in the photograph.

Prohibited Uses

- The iPad is a tool designed to enhance the learning for children. The classroom iPads should only be used for work-related purposes. *(Applies to teachers)*
- The classroom iPads should not be used for personal interests e.g. games and videos (unless these are educational related apps). *(Applies to teachers)*
- Social networking such as Facebook and Twitter are strictly prohibited when using the schools internet on premises.
- Internet content is monitored through the schools proxy. Any inappropriate websites will be flagged and is subject to the schools E-Safety policy.

iPad Settings

- The iPad(s) you have been assigned to has a specific name for a reason. This should not be changed under any circumstances as it is required by the server.
- Before downloading and installing any apps, they should be agreed with by the IT Co-Ordinator.
- Your assigned work email should only be used to download apps onto the iPad. As the iPad is school property it is strictly prohibited to use your personal email.
- iCloud is off limits. You should not be using either a work or personal email for this service as it can cause problems when resetting the iPad for a different member of staff.
- It is your responsibility to keep the iPad up-to-date. When updates become available it is pretty self-explanatory and in doing so you protect the iPad from any software vulnerabilities.

iPad Equipment

- All iPads are issued with a USB cable, cover and charger.
- iPad(s), cover(s), USB cable(s) and charger(s) should remain with the iPad(s) it came with.

Lost, Damaged or Stolen

- If the iPad is lost, stolen or damaged, the IT Co-Ordinator or Head teacher must be informed immediately so that the relevant action can be taken.
- Users should not be lending or giving any iPads and its peripherals to other staff as they will be liable should anything happen to the iPad and its equipment. This may result in a charge being incurred.

Please read the above carefully and sign below:

Failure to take reasonable care or abide by the conditions listed in this document may result in the iPad being reclaimed.

I have read, understand and agree to abide by the terms of the Wexham Court Primary School **iPad Policy.**

Signature:

……

Please Print Name:

……

Date:

……