



Policy for E-Safety (including Acceptable Use Policy)

Reviewed Spring 2023 by Jessica Hill
Next Review: Spring 2025 (Biannual review)

1. Introduction

Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including those for computing, bullying, behaviour and for child protection. The school has appointed E-Safety Coordinators. These are Rachel Cook (Headteacher and designated Children Protection Coordinator) and Amy Newport/Jessica Hill (E-Safety Coordinator/ maternity cover E-safety Coordinator). There is also a designated link governor for E-safety (Carole Williams).

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed bi-annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It is used to raise the standards of education, support professional work of staff and enhance the school's management. Primarily, it is used to promote pupil achievement.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include but are not limited to:

- The Internet – World Wide Web
- E-mail
- Instant messaging (e.g. Snapchat, Viber, Viber, Kik)
- Web based voice and video calling (e.g. Skype, facetime, Whatsapp, Omegle)
- Online chat rooms
- Online discussion forums
- Social networking sites and apps(e.g. Facebook, Whatsapp, Snapchat, TikTok)
- Blogs and Micro-blogs (e.g. Twitter).
- Gaming platforms (Discord/ PS4/PS5/ XBOX).
- Podcasting (radio / audio broadcasts downloaded to devices)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging, apps and internet access

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum and schemes of work. At the start of each computing lesson, pupils from KS1-KS2 receive an e-safety top-tip created by Education for a Connected World which teaches them the importance about staying safe online.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors and DSL's, aims to embed safe practices into the culture of the school.

Leadership team

The SMT ensures that the Policy is implemented across the school via the usual school monitoring procedures, including pupil voice.

E-Safety Coordinator

Our school E-Safety Coordinator is Rachel Cook (Headteacher). She is responsible for keeping up to date on all E-Safety issues and ensuring that staff are updated as necessary. Amy Newport is the second coordinator for E-safety (Jessica Hill is temporarily covering whilst Amy Newport is on maternity leave). Staff and governors receive regular E-safety top tips via monthly emails/ when an issue arises. This keeps staff abreast with any current changes/ updates regarding online safety.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Staff ensure they are familiar with the school E-Safety policy, and ask for clarification where needed.

Class teachers ensure that pupils are aware of the E-Safety rules, introducing them at the beginning of each new school year and embedding them throughout the daily curriculum.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with E-Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school and sign to say they accept these (please see Appendix 1 and Appendix 2).

Parents

Parents are given information about the school's E-safety policy at the admission interview. They are given copies of the pupil information and asked to support these rules with their children. As appropriate they are also sent E-safety top tips via email or text or on the school website every fortnight. This is to address any current E-safety topics that may be presenting themselves either in school or in the media. If an E-Safety issue has arisen with a particular group of children or year group, then communication is made with the relevant parents.

4. Internet Use & Management

Within Telford and Wrekin, Senso monitoring software is used throughout the authority and runs behind every software application. All users must read and sign the 'Acceptable Use Policy- Staff and Governors (Appendix 3) before using any school ICT resources. Senso is designed to protect users and will alert the Headteacher and School Business Manager of any potential breaches of the internet use policy which are then investigated and appropriate action is undertaken. (Screenshots are taken by the software at any instance of violation to allow easy tracking of the site/words used/user and computer involved).

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor TAW can accept liability for the material accessed, or any consequences of Internet access.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. At Key stage 2, children accessing the internet are closely monitored.

5. E-safety Education

Users are informed that network and Internet use is monitored and traced to the individual user. E-safety resources are used within school to teach children safe use of the internet. These resources are regularly updated, as the Internet and use of the Internet is constantly evolving. E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. In year 6 children have a session with a local police officer on E-safety issues.

Newdale uses a range of materials including the CE-OP website which includes a series of child-friendly lessons specifically catered to and differentiated for each Key Stage/Year group to teach them about all elements of E-safety. Integrated into this is an annual Safer Internet Day (February) dedicated to educating the children around the dangers surrounding internet/digital device use. This comprises of key stage assemblies (age-related) and is followed up by lessons to reinforce the messages. Other assemblies dedicated to E-safety are taught throughout the year, often by the Safeguarding Champions team.

Teachers follow objectives for their year group which have been outlined in the 'Educating for a Connected World' (<https://www.gov.uk/government/publications/education-for-a-connected-world>) Government document. The objectives can be met through E-safety/ computing lessons, safer internet day, Share Aware week, NSPCC Speak Out, Stay Safe, Healthy Lifestyles week and during life lessons. At our school E-safety is weaved throughout the curriculum and everyday classroom life.

Pupil voice is often carried out to ensure that we remain up-to-date with the apps and ways in which our children use the Internet. The annual Bullying Survey, carried out in each year group, includes questions around all forms of bullying including that of the dangers of the internet. This ensures that we are clear of the pupils' understanding around this area and in turn can take steps and measures to further educate where necessary. We also ensure that at least one question on the annual Parent survey is linked to E-safety so we can allow parent to have their say.

6. Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum. We teach all our pupils how to find appropriate information on the Internet, and how to ensure as far as possible, that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
- Children are taught how to use search engines (such as Kiddle & Kidrex) and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation

- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

7. Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area: Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES <http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART tips:

- **S**afe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- **M**eeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- **A**ccepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- **R**emember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- **T**ell your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

'It is essential that children are safeguarded from potentially harmful and inappropriate online material. We aim to protect and educate pupils, students, and staff in their use of technology and establish mechanisms to identify, intervene in and escalate any concerns where appropriate.' **Keeping Children Safe In Education 2022**

Staff are aware of the breadth of issues classified within online safety and understand that it is consistently evolving. Staff receive regular CPD linked to E-safety via the E-safety Lead and follow the E-safety risk assessment daily. The risk assessment is categorised into four areas of risk (content, contact, conduct and commerce) . This risk assessment highlights those risks and the measures in place to reduce this risk. All staff in our setting have access to and are aware of this risk assessment.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report

such experiences directly to a trusted adult at the time they occur, so that action can be taken. The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the gold technician (ICT administrator).
3. Logging the incident
4. Discussion with the pupil (and their parent) about the incident, and how to avoid similar experiences in future.

8. E-mail

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

Pupils are taught not to reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission. They are encouraged to immediately tell a teacher if they receive offensive e-mail. The forwarding of chain letters is not permitted.

9. Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets, iPads and games consoles.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school. If this is the case, mobile phones are taken to the school office and kept locked away until the end of the school day, where they are returned to the child. Consent via a parent/ carer must be completed in order for this to happen.

10. Published content and the school web site

The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information is not published, however each year group have an email address in which the parents can email for communication with the teachers and teaching assistants. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

11. Publishing pupil's images and work

Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site. A log is kept of children who we do not have permission to use their photographs and this log is updated regularly. Pupils' full names will not be used anywhere on the Web site or Blog if prior consent has not been obtained, particularly in association with photographs. Pupils work may be published on the website.

12. Social networking and personal publishing

The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind that may identify them or their location whilst on the internet at school or home. Pupils and parents will be advised that the use of social network spaces outside

school is inappropriate for primary aged pupils. Pupil voice surveys often gives us the opportunity to find out what social networking sites the children are currently using so that staff can receive training about these sites if necessary.

13. Managing emerging technologies

Emerging technologies are examined by Telford and Wrekin ICT support for educational benefit and a risk assessment will be carried out before use in school is allowed.

14. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

15. Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom.

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse. Sesno will capture any inappropriate searches and report instantly to the DSL.

Sanctions will include:

Unsuitable material: (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Banning from out of school hours Internet facilities
- Report to Headteacher
- Letter to parent/carer

Offensive material: (e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement
- Removal of Out of School Hours access to Internet

16. Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Whilst it is the duty of the school to ensure that every child in our care is safe, the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, means it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences as a result of accessing the Internet.

17. Use of the Internet and ICT resources by school staff

The Internet

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides a T&W user account that gives further access to specific resources, online tools and email.

ICT Equipment and Resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, digital cameras, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use

Staff are expected to model appropriate ICT and Internet use at all times (please see the Acceptable Use Policy – Staff and Governors- Appendix 3). This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or CPD in using ICT as part of their professional practice can ask for support from the computing Coordinator or the school's Technology support (gold technician).

Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the Headteacher. The appropriate forms and agreements must be signed.

However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements. As with discussion groups, staff are reminded

that professional standards should apply to all postings and messages.

Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

This policy has been written by Rachel Cook , Amy Newport and Jessica Hill in consultation with SMT, Staff and governors.

Review: Next policy review planned for Spring 2025.

Appendix 1- Acceptable Use Policy (EYFS and KS1)



Acceptable Use Policy for EYFS and KS1 children at Newdale Primary School

This agreement will help keep me safe and help me to be fair to others.

- I will always keep my passwords a secret.
- I will ask a teacher or suitable adult if I want to use the computers/iPads/Chrome Books.
- I will only visit sites which my teacher/ a suitable adult has told me are appropriate to use.
- I will take care of computers/iPads/ Chrome Books and other equipment.
- I will ask for help from a teacher/suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me/ makes me feel unsafe on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/iPad/Chrome Book in school.

I am aware that anything I do on the computer may be seen by someone else. I am also aware that the school's internet and safety filter is maintained and monitored by Telford and Wrekin Local authority.

Pupil name:

Signed (child):

Date:.....

Some of the above information was provided by SWGfL.



Newdale Primary and Nursery School E-safety Parental Consent Form

Parent / carer name:.....

Pupil name:

- As the parent or legal guardian of the above pupil, I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I understand that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my child will be informed, if the rules have to be changed during the school year.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.
- I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my child's e-safety or online behaviour. I will support the school at home by promoting safe use of the Internet and technology and I will inform the school if I have any concerns surrounding online safety.
- I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community.

Parent/ carer signature:.....

Date:.....

Some of the above information was provided by SWGFL.

Appendix 2- Acceptable Use Policy (KS2)



Acceptable Use Policy for KS2 children at Newdale Primary School This agreement will help keep me safe and help me to be fair to others.

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes game add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
9. ***I communicate and collaborate online via messaging or email*** – with people I already know and have met in real life or that a trusted adult knows about. I will never meet a real stranger.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, website or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, school, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, websites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

23. ***I use my mobile phone responsibly*** -I will hand my mobile phone to the office in the morning and collect in the afternoon after the school day has ended. My mobile phone number is only ever given to friends I know in real life.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult.

Inside school, my trusted adults

are _____

Outside school, my trusted adults

are _____

Signed: _____

Date: _____

Some of the above information was provided by SWGfL.

Appendix 3- Acceptable Use Policy- Staff and Governor



Acceptable Use Policy – Staff and Governors (Devices)

Newdale Primary School has created this agreement to ensure that staff and governors understand their responsibilities when using school-owned devices, such as mobile phones and tablets, whether on or off the school premises.

Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school

Newdale Primary School retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not fulfil the requirements of this agreement.

Under this agreement, the school will:

- Provide devices for your sole use while you are a permanent/ part-time teacher or HLTA at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the **gold technician** employed by Telford and Wrekin, has installed the necessary security measures on any school-owned device before your use – including, but not limited to, the following:
 - Firewalls
 - Malware protection
 - User privileges
 - Filtering systems
 - Password protection and encryption
 - Mail security technology
 - Tracking technology
- Ensure that all devices undergo the following regular checks and updates by the **gold technician**, including:
 - **Termly** updates to malware protection
 - **Termly** software updates
 - **Annual** password re-set requirements
 - **Termly** checks to detect any unchanged default passwords
 - Malware scans in line with specific requirements

- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.
- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

Under this agreement, you will:

Overall use and care of school-owned devices

- Bring the device (laptop/ computer) and charging unit to the school each day and keep the device with you, or within your sight, at all times.
- Transport the device (laptop) safely and appropriately.
- Not permit any other individual to use the device (laptop) without your supervision, unless agreed by the headteacher.
- Take responsibility for any other individual using the device (laptop).
- Provide suitable care for the device (laptop) at all times and not do anything that would permanently alter it in any way.
- Lock the device (laptop) screen when not in use with a passcode.
- Keep the device clean.
- Store devices (such as mobile phones) in a lockable cupboard located in the staffroom or classroom during lesson times.
- Ensure all devices (home devices such as iPads, laptops, mobile phones) are switched off or set to silent mode during school hours.
- Immediately report any damage or loss of the device (laptop) to the **gold technician**.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the **gold technician**.
- Be prepared to cover the insurance excess, repair or replacement of the device (laptop) when the damage or loss has been a result of your own negligence.
- Make arrangements for the return of the device (laptop) and passcode to the **gold technician** if your employment ends or if you will be away from the school for more than one month.

Using school-owned and personal devices

- Only use the devices (laptop/ school mobile phone) that have been permitted for your use by the headteacher.
- Only use devices (laptop) for educational purposes.
- Only use apps that are compliant with data protection legislation and from reputable sources.
- Ensure that any personal data is stored in line with data protection legislation.

- Only store sensitive personal data on your device (laptop) where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device (laptop) is encrypted and pseudonymised.
- Give permission for the **gold technician** to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the **gold technician**.
- Not install any software onto your device (laptop) unless instructed to do so by the **gold technician** or headteacher.
- Ensure your device (laptop) is protected by anti-virus software installed by the **gold technician** and that this is checked on a weekly basis.
- Not use your device (mobile phone/iPad/ home laptop) to take images or videos of pupils, staff or parents unless permission has been granted from the headteacher.
- Not store any images or videos of pupils, staff or parents on your device (laptop/ mobile phone, iPad/ computer) unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- Not use your school devices (laptop, iPad, mobile phone) to communicate with pupils or parents, unless last resort and permission has been sought from the headteacher.
- Not use your device (laptop/ mobile phone/iPad/ computer) to send any inappropriate messages, images or recordings whilst on the school premises.
- Ensure that your device (laptop/ mobile phone/iPad/ computer) does not contain inappropriate or illegal content.
- Immediately report any illegal, inappropriate or harmful material or incident to the appropriate person.
- Only access social media sites as approved by the headteacher on your device (laptop/ mobile phone/iPad/ computer). Please note only the office staff and senior leaders have access to the school's Facebook page account, or may visit social media sites for online searches as part of the safer recruitment process. Staff are not permitted to go on their personal social media account on a school device.
- The teams of staff referred to above, must follow the staff/ governor code of conduct when on any social media sites.
- Staff are encouraged to set their personal social media accounts to private.

- If members of staff connect their personal device with the school's Wi-Fi, staff must ensure that they follow the staff/governor code of conduct and are not accessing inappropriate content.
- Allow the **gold technician** to monitor your usage of your school device (laptop), such as internet access, and understand the consequences if you breach the terms of this agreement.

*Insurance cover provides protection from the standard risks whilst the device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave the device unattended, and it is stolen, you may be liable for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

Staff agreement

By signing the below, I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed		Date	
Print name		Device model and number	

Headteacher approval

Signed		Date	
Print name			