



# Online Safety Policy

Policy agreed: December 2022

Policy review date: November 2025

Approved by: Headteacher, ICT Link Governor  
and Policy Governor 7.12.22

## **Contents**

1. Introduction
2. Safeguarding and Policy Outline
3. Scope of the Policy
4. Roles and Responsibilities
5. Using the Internet
6. Passwords
7. Expectations of pupils when using the Internet
8. Reporting Procedures
9. Online Safety in the Curriculum
10. Laptops and Tablets
11. Mobile phones/Video Recording
12. Social Media
13. Staff Responsibilities
14. The School Website

## **Appendices**

Appendix A: Internet Access Consent Form

Appendix B: Rules for Acceptable and Responsible Internet Use (Pupils)

Appendix C: Website Photograph Permission Letter

Appendix D: Staff Laptop Computers Loan Agreement

Appendix E: Online Safety Concern Form

Appendix F: School Newsletter Online Safety Tips for Parents

Computing Leader: Miss. Sam Smith

Online Safety Leader: Mr. Jack Orton

Designated Safeguarding Lead and Deputy Headteacher: Mrs. Natalie Harris

Online Safety Governor: Miss. Clare Kenny

## **1. Introduction**

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers need to plan and integrate the use of communications technology such as web-based resources, email and use of tablets and smart phones in to weekly practice. Computer skills are vital to access life-long learning and employment in our ever-advancing technologically driven world.

While all technology carries great benefits, it also presents risks. Internet use is expanding in all sections of society including being used within the classroom environment. This brings young people in to contact with a wide variety of influences, some of which may be unsuitable, on a daily basis. This policy will outline how all members of Walmley Junior School will adopt strategies to for the safe and responsible use of the internet and any advancing and emerging technology that children may have access to.

## **2. Safeguarding**

Safeguarding is defined as –

- Protecting children from maltreatment;
- Preventing impairment of children's health or development;
- Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care; and
- Taking action to enable all children to have the best life chances.

Walmley Junior School is committed to safeguarding and promoting the welfare of all its pupils/students. We believe that:

- All children/young people have the right to be protected from harm;
- Children/young people need to be safe and to feel safe in school;
- Children/young people need support which matches their individual needs, including those who may have experienced abuse;
- All children/young people have the right to speak freely and voice their values and beliefs;
- All children/young people must be encouraged to respect each other's values and support each other;
- All children/young people have the right to be supported to meet their emotional, and social needs as well as their educational needs – a happy healthy sociable child/young person will achieve better educationally;
- Schools can and do contribute to the prevention of abuse, victimisation, bullying, exploitation, extreme behaviours, discriminatory views and risk taking behaviours; and
- All staff and visitors have an important role to play in safeguarding children and protecting them from abuse.

The Online Safety Policy will be used in conjunction with other mandatory policies; Safeguarding and Child Protection Policy and the Data Protection Policy.

### **The purpose of this policy is to:**

- Establish the ground rules we have in school for using the internet.
- Demonstrate the methods used to protect children from unsuitable online content outlining the school's acceptable use policy.

- Set out the curriculum requirements with regards to Online Safety.
- Establish responsibilities amongst staff and pupils with regards to the use of technology including smart phones and tablet computers.

The school believes that the benefits of accessing resources via the internet, far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, is one the school shares with parents and guardians.

We believe that the best recipe for success lies in a combination of site-filtering, of supervision, education, awareness and by fostering the responsible attitude in our pupils in partnership with their parents and/or guardians.

As part of annual transition from our Infant school, parents are sent an explanatory letter and the rules which form our Acceptable and Responsible Internet Use Agreement (See Appendix A & B). This agreement is signed by both the parents and the pupils and returned to school in September. These agreements are stored in the school office. In addition, the parents are requested to state whether their child's photograph can appear on our school website and social media (See Appendix C). These forms are stored in the school office.

### **3. Scope of the Policy**

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers and visitors) who have access to and are users of school digital technology systems, both in and out of school.

### **4. Roles and Responsibilities**

#### **Headteacher and Senior Leaders**

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

#### **Governors**

The school governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Safeguarding Governor, Miss Kenny, has taken the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Online Safety Lead
- Receiving feedback and updates from the Online Safety Council
- Regular monitoring of online safety logs
- Reporting to Governors

#### **Online Safety Lead**

- The Online Safety Lead will lead the Online Safety Council.
- They will also take day to day responsibility for online safety issues and has a role in reviewing school online safety policies.
- They will ensure that all staff are aware of the procedures that need to be followed when an online safety incident takes place.
- Provide training and advice for staff.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Liaises with relevant Governor to discuss current issues.
- Reports regularly to Senior Leadership Team.

### **Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current Online Safety Policy.
- They have read, understood and signed the Staff Acceptable Use Policy.
- They report and suspected misuse or problem to the Head Teacher/Senior Leader or Online Safety Lead for investigation.
- As part of a whole school approach to Online Safety, handle Online Safety concerns themselves and inform the Online Safety lead or Head Teacher as appropriate.
- All digital communications should be on a professional level and only carried out using official school systems.
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism.
- They monitor the use of digital technologies in lessons.
- Guide pupils to suitable websites that are suitable for their use.

### **Online Safety Council**

The Online Safety Council provides a consultative group that has representation from children across the school, with responsibility for issues regarding online safety. Members of the Online Safety Council will assist the Online Safety Lead with the following:

- Raising awareness of online safety within school.
- Delivering half termly tips to help children stay safe online.
- Delivering online safety messages in whole school assemblies.
- Assisting the Online Safety Lead during Safer Internet Week.

### **Pupils**

- Are responsible for using school digital technology in accordance with the Pupil Acceptable Use Agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate content and know how to do so.
- Should understand the importance of adopting good online safety practice when using technology out of school and understand the Online Safety Policy covers their action out of school.

## Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website and Twitter. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in school

## 5. Using the Internet

The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries and museums.
- Rapid and cost effective worldwide communication.
- Gaining an understanding of people and cultures around the globe.
- Staff professional development through access to new curriculum materials, experts' knowledge and practice.
- Exchange of curriculum and administration data with Local Authority/Department for Education and Skills.
- Social and leisure use.
- Greatly increased skills in Literacy, particularly in being able to read and appraise.

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons across all areas of the curriculum.

All staff will be asked to review and evaluate resources available on websites appropriate to the age range and ability of the pupils being taught and then share this information with members of the team; building up a repertoire of sites to call upon during lessons.

Initially the pupils may be restricted to sites which have been reviewed and selected for specific content. They may be given tasks to perform using a specific group of web sites until they are used to 'free searching' using one or more recognised search engines.

As pupils gain experience, they will be taught how to use searching techniques to locate and specific information for themselves. Comparisons will be made between researching from different sources of information. We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located.

The current filtering service is managed by the Birmingham Grid for Learning (BGFL) and Link2ICT who will block unsuitable web pages based on a database defined by the Government. These sites can be amended by the school where necessary enabling a more comprehensive blocking service; one that is suited and created by Walmley Junior School.

## 6. Passwords

All members of the school community (staff and pupils) are given passwords to access school digital technology. Pupils are taught and made aware that their password is to be kept safe and is an important part of keeping their personal details private. If a pupil password is forgotten, the

school I.T technician has the ability to reset that password so that a child can access school technology.

## **7. Expectations of pupils when using the Internet**

At Walmley Junior School we have many ways of monitoring the children's use of the internet facilities provided in school (including Earlybirds) and minimise the chances of pupils encountering undesirable material.

All pupils are expected to read and agree the Acceptable Use Agreement. This agreement appears on the computer screen each time any user logs on and is part of our Smoothwall Software for monitoring computer use. The children's parents will have already returned a signed Internet Access Consent Form when their children start their education at Walmley (See Appendix A). We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and the language that they choose to use.

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 teacher, so that the Service Provider can block further access to the site.
- To ask permission before accessing the Internet and have a clear idea why they are using it.
- Not to access other people's files unless permission has been given.
- To use computers for schoolwork and homework only unless permission has been granted otherwise (during free time perhaps).
- Not to download files to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- Not to give out personal information such as phone numbers and addresses when using technology.
- To remain on the sites provided to them or use the appropriate search engines in order to reach desirable, appropriate web content.
- Access to personal accounts online is prohibited. However, in certain circumstances, the children are given permission to access said accounts. For example: Code.org programming website – the children can access their accounts so that they can work on a project that they have been working on at home. This will be monitored by the teacher using Veyon Master software in the Computing room.

Pupils choosing not to comply with these expectations will be warned, and subsequently, if further instances occur, will be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a letter to parents and withdrawal of privileges.

## **8. Reporting Procedures**

Walmley Junior School will only allow children to use the Internet when there is a responsible adult present to supervise. Pupils will be directed to websites by staff that will have checked out the suitability beforehand. If a URL is encountered that is deemed to be inappropriate then the member of staff should report this to the Computing Leader or the Headteacher who will investigate and refer to the appropriate authorities for the URL to be added to the list of blocked sites.



Within school (including Earlybirds), all computer users have unique logins and are monitored by the software 'Smoothwall' which takes screenshots of unsuitable content. If there is an issue, flagged up by Smoothwall, the Computing Leader and Headteacher will investigate the content reported. At Walmley Junior School, the Online Safety Lead regularly checks the screenshots taken from pupils' screens and reports any concerns immediately to the Headteacher. The Headteacher monitors the screenshots taken from teachers' screens. These screenshots occur when using the internet as well as when any user is logged on to the school system or using the various software required within lessons. These records are kept in the Safeguarding Folder 1 in the Headteacher's Office.

Should improper use of other technology be witnessed, such as when using iPads, the class teacher will inform the senior leadership team (SLT) and together decide on what the consequence will be; this could include a technology access ban for the child in question.

Any issues that are raised, via Smoothwall, class teacher, by the children themselves or parents/carers will be logged in the Online Safety Concern folder, situated in the Headteacher's Office. Should multiple issues occur over a child's time at Walmley Junior School then this will be referred, by the headteacher or SLT, to the child's parents; where the school will then work in partnership with the parents to resolve the issue at hand. This folder will also contain technology based issues from outside of school, brought to the school's attention by parents from outside of school. These may relate to messages received through social messaging sites and through mobile phone contact outside of school.

Any incidents or complaints of a child protection nature must be dealt with in accordance with the school Safeguarding Policy. Children, parents and staff can report any online abuse via the CEOP link on the school website: <http://www.walmley-jun.bham.sch.uk/> or by completing the Online Safety Concern Form (Appendix E) which is automatically forwarded to the Online Safety Lead.

Keeping children safe in education 2022 and our School behaviour policy state that we don't condone child on child abuse. Action is always taken against bullying (including cyberbullying and sexting), physical, sexual and verbal abuse. Watching or doing nothing can suggest support for unacceptable behaviour. Racism is unacceptable at Walmley Junior School. All forms of peer on peer abuse must be addressed without delay and reported to the Headteacher so it can be logged and dealt with accordingly.

If an adult suspects that their child is being bullied online, they should remember to report as listed above.

## **9. Online Safety in the Curriculum**

Walmley Junior School is proud of its Online Safety provisions and will educate all children within our care to be responsible users of technology. This will be in the form of:

- Half termly Online Safety lessons are taught during class assemblies or PSHE. Planning for this is differentiated for year groups and available in year group folders, and includes various issues from generating passwords to using online games. During Safer Internet Week, a whole school assembly will focus on various issues of Online Safety and extended activities will be delivered in class.
- Children's attention should be drawn to the SMART rules each lesson, which are displayed in the Computing suite, along with other Online Safety information produced by pupils.

We are also very careful about our own personal information and of the information that is stored on SIMs.

SIMs allows class teachers to take online registration enabling instant and up to date records for office staff on the attendance of pupils. SIMs also allows access to personal data of pupils such as attendance information, emergency contact details and address information. It is therefore vitally important that when staff use this system they logout once registration is complete. Staff must never allow children access to the system unattended and must never divulge the username/password to pupils.

The school will also provide parents with up-to-date information with regards to Online Safety via newsletters, information given at parents' evening (including a list of informative websites), the school website and Online Safety workshops (when available).

The Online Safety Policy sets out the use, monitoring and reporting of technology provided in school. Online Safety best practice and guidance is encouraged outside of the school for use on mobile devices owned by pupils and in the home.

## **10. Staff Laptop**

Teaching staff are allocated a laptop for PPA and teaching purposes.

- The laptop can be connected to the internet out of school but must be used for school business.
- Staff laptops will be returned to the school ICT technician regularly for critical updates and software installations.
- Information, with regards to children, should be stored on the Staffcommon drive (J:) so that the only people who can access it are those who have staff permissions.
- All staff sign a Laptop Computer Loan Agreement (Appendix D).
- All staff have a copy of the Code of Conduct Policy November 2021. Section 17 refers to the unacceptable use of ICT facilities and monitoring.

Walmley Junior School has access to Apple iPads. These are to be used inside school for curriculum based tasks only. If photographs are taken during a lesson, it is the responsibility of the class teacher to remove them once they have been used for what was intended. The photographs will be stored in a secure location on the staffcommon (J:).

When choosing new apps and software to download on to the tablets, the Computing Manager and the ICT technician will be instructed to do so. These apps will first be checked for suitability and appropriateness before being shared with the children.

## **11. Mobile Phones/Video Recording and Cameras**

11.1 Unfortunately, there are currently now instances of mobile phone camera images and messages (texting or via social media) being used inappropriately to bully children in other schools. This policy will hopefully prevent such issues affecting our school. It is the school expectation that children do not have access to mobile phones or bring them to school unless they walk to and/or from school. Children should be reminded that they should not use their mobile phone in school to take photographs, selfies or have conversations with other children. Children should hand them in to the school office for safe keeping throughout the day and have them returned at the end of the school day. All phones are left at the owners' risk – the school

accepts no responsibility for mobile phones. Also, children should not take a mobile phone on school trips or residential.

### 11.2 Adults

There are situations in schools where adults have been accused of taking photographs of children using their mobile phones, thus creating child protection issues. To protect staff from such allegations and to maintain professional standards, this policy will satisfy these issues.

Staff are allowed to bring mobile phones on site, but must be turned off/be on silent mode and not visible in any area where children could usually appear (i.e. classrooms, halls, library, school office, playgrounds and ICT suites). Phones can be kept on silent, but should be kept in a locked bag or cupboard, in order to protect it from theft.

Under exceptional circumstances, a member of staff can request that their phone be turned on and accessible/ visible during the school day. Such a case needs to be discussed with the Headteacher.

During breaks staff are obviously allowed to check their phones and make calls if necessary, but this must be in areas where children would not be able to enter (i.e. a classroom with the door closed, the Earlybirds Office or the Technology Room). This does not include shared areas where children may overhear.

Adults should use equipment provided or authorised by the School to make/take images and should not use personal equipment, mobile telephones or any other similar devices to make/take images unless authorised by the Headteacher. For example, to upload and share photographs with parents via Twitter during school trips. The images should be transferred to the school network as soon as possible.

As stated in the Code of Conduct Policy November 2021 (Section 16), the following guidance should be followed:

- if a photograph is used, avoid naming the pupil
- if the pupil is named, avoid using the photograph
- photographs/images must be securely stored and used only by those authorised to do so (on the school network as soon as possible)
- be clear about the purpose of the activity and about what will happen to the photographs/images when the lesson/activity is concluded
- only retain images when there is a clear and agreed purpose for doing so
- ensure that a senior member of staff is aware that the photography/image equipment is being used and for what purpose
- ensure that all photographs/images are available for scrutiny in order to screen for acceptability
- be able to justify the photographs/images made
- do not take images of pupils for personal use
- only take images where the pupil consents to this
- do not take photographs in one to one situations
- do not display or distribute photographs/images of pupils unless there is consent to do so

from the parent/carer

- only publish images of pupils where they and their parent/carer have given explicit written consent to do so
- do not take images of pupils in a state of undress or semi-undress
- do not take images of pupils which could be considered as indecent or sexual.

### **11.3 Visitors and Parents**

All visitors should likewise follow this policy and if a member of staff is concerned about their use of their mobile phone, or has a child reported a concern, please inform a senior leader immediately, who will then request to examine the phone.

Some engineers (e.g. contractors) as part of the contract with the school are permitted to carry mobile phones, in order to photograph their working conditions. This is agreed beforehand, but nonetheless any concerns must be reported and a senior leader is allowed to search the phone for images. Likewise, the Site Supervisor is also allowed to carry mobile phones, but should wherever possible, answer the phone in a private place. Out of professional courtesy, mobile phones should be turned off during staff meetings, unless an agreement has been made with the Headteacher.

### **11.4 Mobile Phones on Trips**

On a normal school day trip, it is expected that staff will carry a mobile phone. If the year group are going away for more than one day or are spread over 2 coaches, then it is understood that staff would need to take their own phones to stay in touch with each other. In this circumstance to protect the staff members it is important to consider where and how you are using your phone. It may be advisable to use the phone near to another member of staff/adult if children are present, or to make the phone call away from the children, whilst making sure that the children are still supervised by a member of staff.

### **11.5 Video Recording and Cameras**

In order to protect staff from any sort of allegation, staff should not use their own cameras or video cameras to record the children in school. Each Year Group have been issued with a school camera that they are responsible for, and these should always be used (Code of Conduct Policy November 2016, Section 16).

Images once used or printed should be removed from laptops, tablets and cameras or stored centrally on the school system. Whenever taking photographs, staff must always check the register of pupils who have been refused permission by their parents to have photographs taken of them. This register is kept in the school office.

During Christmas and special performances, the school currently allows parents to photograph and video children but ask for these not to be shared on social media. To date, we have not received any complaints regarding parents uploading video clips etc. of pupils in performance on social media.

## **12. Social Media**

School social media accounts (e.g. Twitter) must be monitored regularly and kept up to date. Digital communications by staff must be professional and respectful at all times and in accordance with this policy. School social media accounts must not be used for personal gain and must ensure that confidentiality is maintained even after they leave the employment of the

school. Unacceptable conduct will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate. The tone of content published on school social media should be engaging, conversational, informative and friendly.

### **13. Staff Responsibilities**

- Personal Data will be stored securely and will be restricted to staff members who need the information (Code of Conduct Policy November 2021, Section 3)
- Confidential data will be stored on the staff shared area to which only fulltime staff will have access.
- All staff will have a user account and understand the importance of a secure and strong password.
- Only Admin staff and SLT will have access to CMIS/SIMS and accounts information.
- Staff will only have access to CMIS/SIMS if their role requires it.
- CMIS/SIMS access will be restricted for all users allowing them to view the data to which they are entitled.
- Access to the Admin network will be restricted for all users other than Admin staff.
- Personal Data will not be stored on shared drives to which children have access.
- Data that can identify an individual should not be stored on staff laptops or offsite, and staff should be aware of the responsibility they have in minimising the risk for this data to be obtained by third parties in accordance with the Laptop Computer Loan Agreement.
- Members of staff are issued with encrypted laptops for data storage but personal data is not endorsed.
- It is the responsibility of all staff members to ensure that the children are adhering to the protocols outlined in this policy. They will follow the correct procedures should issues arise.
- Any incidents or complaints about staff misuse must be referred to the headteacher.

### **14. The School Website**

Our school website will celebrate good work, promote the school, inform parents of up and coming events, publish resources for projects/homework and link to other good sites of interest.

Information published will be accurate as at date of publish, and any inaccuracies that may occur will be corrected as soon as is possible.

Where photographs of pupils are to be uploaded then agreement will be made with parents and names will not be published. Files uploaded will not refer to names. E.g. A photo of Joe Bloggs will not be joebloggs.jpg.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. This is done before the children arrive in school as parents are asked to sign and return a website photo permission letter (See Appendix C).

Group photographs will not contain a names list. Display will be of the highest quality and reflect the status of the school. Home information and e-mail identities will not be included only the point of contact to the school i.e. phone number, school address and all emails will be submittable through on site forms, no email address will be posted on the website.



Dear Parents/Carers,

**Internet Access for Pupils**

As part of the schools I.T. programme we will be including supervised pupil access to the Internet, the global network of computers you will have read about and seen on television. Before the school allows pupils to use the Internet, they must obtain parental permission. Both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Various projects have proven the massive educational benefits of Internet access, which will enable pupils to explore thousands of libraries, databases and bulletin boards. They will also be able to exchange messages with other learners and teachers throughout the world. Although Internet use is supervised in our school, families will wish to be aware that some pupils may find ways to access material which is inaccurate, defamatory, illegal or potentially offensive to some people. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. However, as with any other area, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. The school therefore supports and respects each family's right to decide whether or not to agree to access.

During school, teachers will guide pupils towards appropriate material. Outside school, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.

If you decide to support your child's application for access to the Internet, please complete the enclosed form and return it to me by the end of term.

Yours sincerely,

Mr. S .Pearson  
Headteacher

.....  
**Please complete and return this form to the Headteacher.**

Pupil .....

As a school user of the Internet, I agree to comply with the school acceptable use rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil's signature .....Date .....

Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Inter net. I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

Parent's signature..... Date .....

Pupil's name .....

Class ..... Home telephone no: .....



**Walmley Junior School Child  
Acceptable Use Agreement  
2019**



Please share and read this Acceptable Use Agreement with your child. It is vital that children use computers and technology responsibly in school.

**SAFE**

- ✓ Walmley Junior School will help me stay safe when I'm using technology in school.
- ✓ I know that Walmley Junior School will monitor my use of technology in school.
- ✓ I will NEVER give my user name and password away to anyone.
- ✓ I will not deliberately type or search for anything that is bad or inappropriate.
- ✓ I will take care of ALL Computing equipment.
- ✓ I am aware that some websites and social networks have age restrictions and I respect this.
- ✓ I will not attempt to visit websites that I know are blocked by the school.

**MEET**

- ✓ If someone tries to talk to me on the computer that I don't know, I will ignore them and tell an adult.
- ✓ I will NOT give out any information about me to strangers at any time (name, address, age, email address, phone number, school).
- ✓ I will be polite and not use nasty or bad words when typing or talking to my friends.

**ACCEPTING**

- ✓ If am not sure about an email, attachment, picture or message, I will tell an adult straight away.
- ✓ I will not click on any pop ups that may appear on my screen.
- ✓ I will only visit sites and play games that are suitable for my age.

**RELIABILITY**

- ✓ I know not all information online is true and I will make sure I check more than one website.

**TELL**

- ✓ If I am worried or upset by something I see on the computer, I will use **Hector the Protector** and tell an adult straight away.
- ✓ I know how to report online abuse to someone in school and how to use the CEOP Report button.

I understand that I must use school technology in a responsible way to ensure that there is no risk to my safety or to other users at Walmley Junior School.

---

**Acceptable Use Agreement 2019**

Signed (Pupil): .....

Class: .....

*I have read and discussed this agreement with my child.*

Signed (Parent/Carer): .....





Appendix C



Dear Parents/Carers,

Photo Permission

We occasionally share photographs of the children taking part in a variety of activities or showing their work. This can be either on our website or for school publicity purposes in local newspapers/online news. This would mean that, if your child is chosen, their images could be viewed publicly.

Please return the slip below as soon as possible indicating your preference with regards to publishing photographs of your child publicly.

Yours sincerely,

Mrs. S. Smith  
Deputy Headteacher

---

Photo Permission

Child's name \_\_\_\_\_ Class \_\_\_\_\_  
(Please tick your preference)

- I give permission for my child's photograph to be used on the school website.
- I do not give permission for my child's photograph to be used on the school website.
- I give permission for my child's photograph to be used for school publicity Purposes (including Twitter)
- I do not give permission for my child's photograph to be used for school publicity purposes (including Twitter).

Signed \_\_\_\_\_ Date: \_\_\_\_\_



## Staff Laptop Computers Loan Agreement

This Loan Agreement is between ..... and Walmley Junior School.

The recipient of Computer Number ..... agrees to the following undertakings with regard to the loan of the laptop computer.

- Insurance of the computer is provided under the School's Insurance Policies. **The computer is not covered if left unattended in a motor vehicle.**
- Installation of additional software other than that provided by the school should only take place by permission of the school.
- The computer remains the property of the school whilst on long-term loan to the teacher.
- Remember that the laptop is for work purposes only and should not be used by friends, family or children.
- Users understand that this laptop will be monitored, both at school and at home, to comply with the school's Safeguarding and Online Safety policies (sec. 7).
- Teachers will not disclose any information relating to school whilst using any other web sites without the written permission of the school.
- Although memory sticks are used for the transportation of documents to and from school, they must never contain delicate information e.g. personal information of children, class list and children's reports.
- The supplied laptop **must** be used when writing reports as the school laptop has built in encryption. Also, this will reduce any formatting issues when sharing the reports with the senior leadership team.

Signed ..... Teacher/TA

Signed ..... Headteacher



**Online Safety Concern Form**

This form is for use by any adult working in school that has a concern about e-safety. This could be a concern after a child has made a disclosure regarding something that has happened when they are using a computer/mobile phone or other electronic device or about being bullied (cyber bullying). It could also be a concern that has been reported by a parent. Your concern may be a general issue about ICT practices in school or social networking sites involving children.

Date:	Time:	Place: home school other
Name of child:		Class
Other adults or children present:		
Description of concern/nature of incident:		
Action taken:		
Signed:	Name: Position:	
Follow up action with parent: police	call	meeting letter
Date:		



## Online Safety Tips for Newsletters

### **ONLINE/SAFEGUARDING TIP OF THE WEEK**

Your password should be like your toothbrush “not shared”!!

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

The kidsmart website is a really good place to play some games and test your internet safety knowledge. You can also pick up some useful tips on staying safe online:

<http://www.kidsmart.org.uk>

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

SMART RULES - S for safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

SMART RULES - M for Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

SMART RULES – A for Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

SMART RULES - R for reliable. Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family.

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

SMART RULES – T for tell. Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

It is never too late to tell someone if something makes you feel unhappy or uncomfortable. Tell a parent or a teacher and they can help you report it to the people that should know.

### **ONLINE SAFETY/SAFEGUARDING TIP OF THE WEEK**

Some social networks appear to be designed for younger audiences. Always read the terms and conditions of use and ensure you are happy and comfortable with what they say. Most allow you to upload pictures but they may then take ownership of them and allow others to use them freely. Always think about what you put online and what others could do with it because once its online, it will probably be there forever!!