



QUINTON HOUSE SCHOOL

Safeguarding: Online Safety Policy

As a school we are committed to keeping our pupils safe in all situations including internet use.

MARCH
2017

CONTENTS

1.0 INTRODUCTION

2.0 WHOLE SCHOOL APPROACH

3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

4.0 STAFF AWARENESS AND TRAINING

5.0 E-SAFETY IN THE CURRICULUM

6.0 INFRASTRUCTURE AND DATA MANAGEMENT

7.0 MONITORING, AUDIT AND POLICY REVIEW

APPENDICES

A) ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

1.0 INTRODUCTION

1.1 We define E-Safety as:-

- ensuring pupil Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring pupils are educated on the risks carried with Internet use and how to minimise and deal with those risks.
- providing pupils with knowledge and resources to make decisions to ensure their safety online.

1.2 Our core principles for E-Safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning
- Our policies seek to educate and inform pupils and the school community on the safe and prudent use of Internet resources
- We take a whole school, consistent approach to E-Safety, recognising that all staff should be involved and clear on their role in ensuring E-Safety education
- E-Safety is subject to clear reporting routines and an age appropriate Acceptable Use of Technology Agreement is in place for all pupils
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise
- Our policy reflects current practice and is regularly reviewed and updated by the Senior Leadership Team and communicated to all staff
- E-Safety is addressed within the curriculum at all ages
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy complements other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and pupil / pupil Acceptable Use of Technology Agreement
- The E-Safety policy is dated with a review date and the SLT has responsibility for ensuring it is reviewed and updated on an annual basis

2.0 WHOLE SCHOOL APPROACH

2.1 We take a consistent approach to E-Safety and ensure that:

- All staff are aware of their responsibilities. E-Safety procedures are discussed in induction for new staff. The policy and procedures are discussed in staff briefings and training is provided at regular intervals.
- We ensure all pupils understand what is meant by E-Safety through age appropriate delivery in the curriculum at all ages.
- All pupils are subject to the Acceptable Use of Technology Agreement (AUTA) which is signed by the pupils on entry to the school.
- Parents are aware of their children's responsibilities under the AUTA and sign the agreement for younger pupils/ pupils.
- Awareness raising events are held, such as assemblies, parents' forums and PCSO/Police visits.
- E-Safety is raised as part of school council discussions.

- There are notices and posters giving guidance on display in key areas of the school.

3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

3.1 We hold an Acceptable Use of Technology Agreement (AUTA) that sets out positive guidelines for how pupils should use and treat technology both during the school day and outside school as school representatives.

3.2. The AUTA sets out guidelines for:

- appropriate and respectful use of school technology equipment and devices
- expectations and regulations for the use of pupils' own devices in school
- expectations of behaviour if equipment is found broken or non-functional
- appropriate communications using devices in and out of school
- code of practice if pupils discover inappropriate or upsetting material on any device
- clear guidance on how to report any concerns

3.3 The AUTA is used positively to encourage appropriate and E-Safe behaviour and can be used alongside rewards for positive use of technology

3.4. The AUTA is supported by a clear set of age appropriate sanctions for behaviour that contradicts the agreement.

3.5 The AUTA is shared with parents and their views are welcomed and considered.

3.6 The AUTA is not intended to form the whole basis of E-Safety education, but to complement discussions and lessons on E-Safety during curriculum time and to provide a robust agreement setting out clear expectations for behaviour.

3.7 The AUTA is designed to be binding for pupils while *enrolled* in the school and the school reserves the right to take action on behaviour that contradicts the Agreement outside of school time. In these cases the school will proceed with discretion and in partnership with parents.

3.8 Pupils, parents and all staff are able to report concerns and guidance for this should be set out in the AUTA.

4.0 STAFF AWARENESS AND TRAINING

4.1 All staff are bound by the code of practice set out in the Cognita Schools Policy for use of Internet and mobile devices. This should be available for all staff and ensures that staff use technology safely and with adherence to safeguarding principles.

4.2 At least one member of staff undertakes accredited training.

4.3 The accredited member of staff provides a higher level of expertise within the school and can guide staff in E-Safety practice and review of E-Safety policy and procedure and provide INSET guidance.

4.4 E-Safety is built into the termly programme of meetings to ensure all staff are aware of their responsibilities and for the discussion of any issues, concerns or opportunities for events or cross curricular E-Safety lessons.

4.5. There is a clear procedure for staff wishing to report or discuss concerns relating to E-Safety or Internet access in the school.

4.6 Staff responsibilities for E-Safety are: (for all staff)

- To ensure they are familiar with and fully support the pupil Acceptable Use of Technology Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of school technology
- To provide reminders and guidance to pupils on acceptable use
- To report and act appropriately if they become aware of, or after any pupil reports, a concern or an incident involving technology use
- To ensure E-Safety is delivered within the curriculum as appropriate to their pupil age range and subject area
- To contribute to and discuss E-Safety policy and to have their views heard
- To be aware of the school policy for tackling bullying and how this relates to incidents of cyber-bullying
- To be mindful of protecting data and keeping access to digital information secure by adhering to the school password policy and protecting their accounts from pupil access
- To use secure portable data options including password protected or encrypted portable memory devices

5.0 E-SAFETY IN THE CURRICULUM

5.1 E-Safety should be embedded into the curriculum at all age ranges. Lessons should be well planned and resourced and there should be a number of opportunities to discuss a range of E-Safety issues.

5.2 E-Safety is expected to be covered within ICT and PSHEE lessons but should not be exclusive to these subject areas and discussion of E-Safety should be explored in other subject areas both while using technology and as a topic as appropriate

5.3 Guidance on minimum coverage in each key stage:-

EYFS – safe and responsible use of technology should be modelled; Suggestions relating to ELG could include:

- Communication and Language – pupils aware that they are able to communicate with others using devices – appropriate language and key words associated with technology
- Physical development – safe and careful handling of technology
- Personal, Social and Emotional development – sharing and cooperating while using technology
- Understanding of the World – awareness of devices around us and how they are used to keep us safe, provide us with information
- EYFS children should be given opportunities to learn collaboratively with devices

Key Stage 1 – Typical KS1 E-Safety coverage should address: Pupils should be made aware of distinction between personal, private and public information. Pupils should be taught appropriate ways to communicate when using devices and how to respond to unpleasant or distressing comments they may encounter online. They should be made aware that people they do not know are strangers including while playing online games and the importance of using ‘usernames’ and guarding against volunteering information. They should be taught how to respond if they are distressed or uncertain about any material they are exposed to while online or using technology.

Key Stage 2 – Issues outlined above should be addressed with the addition of: Importance of passwords and cyber security. Understanding of how cyberbullying is using technology to be unpleasant and guidance on how to respond constructively and report any thing that concerns them. Understanding of how social networks allow sharing of information and the importance of keeping information about themselves private. Understanding of how data submitted to the Internet including photographs, comments, emails etc. can be potentially accessed, altered and used by anyone. Clearer understanding of distinction between private and public information. Discussion of support networks and methods of reporting anything they are uncertain or concerned about. Understanding of spam, unsolicited and scam activity on the Internet and how accounts can be hacked or accessed by criminals.

Key Stage 3 and 4– Issues outlined above are all relevant with the addition of: Discussion of E-Safety issues in the news and current affairs. Understanding of the law and relevant acts passed to protect people from discrimination, abuse and exposure to indecent content. Discussion of how photographs, information and comments posted online can be accessed by any one and cannot be retracted or removed easily. Fuller understanding of how everyday use of technology can be made more secure through intelligent password use, vigilance and due care when using public technology facilities. Understanding of plagiarism and copyright laws. Addictive nature of devices. Access to relevant support networks and guidance on dealing with cyberbullying, peer pressure and social aspects of device use.

5.4 Extra –curricular activities such as Safer Internet Day opportunities, visits from local PSCO, school assemblies should be explored but these should not represent the majority of E-Safety

teaching or discussion in the academic year. They should be used to support lessons embedded in the curriculum.

5.5 Use of mobile devices during 6th form lessons is subject to control and risk management. Expectations of appropriate use of mobile devices are set out in the AUTA for pupils. This includes pupils are expected not to share digital images or videos of other pupils taken during lessons for any purpose other than school use.

5.5 Opportunities for peer mentoring or 'buddy' systems can be explored so that older pupils can act as role models for younger children and provide a further method for pupils to report concerns

6.0 INFRASTRUCTURE AND DATA MANAGEMENT

6.1 The school Internet access is subject to filtering and control and this is updated regularly

6.2 Staff are vigilant during lessons involving Internet access

6.3 Where available, screen watching facilities are used and staff are aware of how to utilise these resources

6.4 Passwords and digital security is in place to protect data and data is managed in accordance with the relevant DP Acts

6.5 Staff are fully aware of how to report a problem or any incidents relating to data security or Internet control

6.6 Professional communications between the school and other organisations or parents take place within clear professional boundaries, are transparent and open to scrutiny and do not share personal information with pupils

7.0 MONITORING, AUDIT AND POLICY REVIEW

7.1 The E-Safety policy is dated and an annual review date is stated

7.2 It may be necessary for more frequent reviews if a number of incidents are recorded.

7.3 The review procedure should be:

- An audit of effectiveness of current practice
- A review of guidance published by relevant organisations
- Amendments to be shared with all staff

7.4 To audit E-Safety effectiveness of the current policy the following questions should be considered:

- Has recording of E-Safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all pupils demonstrate an awareness of E-Safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?

- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording of the Acceptable Use of Technology Agreement fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is E-Safety observed in teaching and present in curriculum planning documents?

Appendix A

INTERNET SAFETY

Quinton House School

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT FOR PUPILS and PARENTS

The document is comprised of this cover page and two sections:

Section A:

- Computer Use Agreement for Quinton House School and Nursery and Internet Safety Rules including explanatory notes for parents

Section B:

- Parent and Pupil Computer Use Agreement Form
-

Instructions for Parents

1. We are sure that as Parents you are only too aware of the way the world of communication has changed. What was unthinkable just a few years ago becomes reality in a flash and keeping up with all the benefits and dangers this brings becomes a challenge. Our firm belief is that the best way of maximising the benefits whilst minimising the dangers is for Parents, Pupils and the School to have a common understanding around the use of ICT.

We would like you to read the Computer Use Agreement and the Internet Safety Rules carefully. If help is needed to understand all the language, or there are any points you would like to discuss with the school, let the school know as soon as possible.

2. Discuss the Internet Safety Rules with your child and think through how you manage this within or outside your home.

3. Both you and your child should sign the Computer Use Agreement Form and return that page to the school office.

4. Please keep Section A for future reference. (The term 'Parent' used throughout this document also refers to legal guardians and caregivers)

Important terms used in this document:

(a) The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
(b) '**School ICT**' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined) below.

(c) The term '**ICT equipment/devices**' used in this document, includes but is not limited to, computers (such as desk tops, laptops, PDAs), storage devices (such as USB, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar technologies as they come into use.

INTERNET SAFETY AND THE SCHOOL COMMUNITY

NOTE: Use of the school’s ICT facilities assumes that pupils have read and accepted this Computer Use Agreement

COMPUTER USE AGREEMENT - ICT Safety Policy at Quinton House School

The values promoted by Quinton House School and Nursery include respect for yourself and others in the school community and a commitment to enabling everyone to achieve their personal best in an environment that is physically and emotionally safe. The measures outlined in this document ensure the internet safety of the school is based on these values.

The school’s computer network, internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Quinton House School and Nursery and to the effective operation of the school. However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

Internet safety use agreements include information about obligations and responsibilities and the nature of possible consequences associated with breaches of the use agreement, which undermine the safety of the school environment. The overall goal of the school in this matter is to help keep the school community safe by creating and maintaining an internet safety culture which is in keeping with the values of the school.

1. ICT Safety Policy

1.1. All staff and pupils, whether or not they presently make use of school ICT, will be issued with a Computer Use Agreement. Parents are asked to read these pages carefully and return the signed Agreement form in Section B to the school office for filing. A copy of this signed form will be provided on request.

1.2. Parents are asked to keep the other pages of the Agreement for later reference

1.3. The school encourages anyone with a query about the Agreement to contact staff.

2. Requirements regarding appropriate use of ICT in the school learning environment

In order to meet the school’s legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

2.1. The use of the school’s computer network, internet access facilities, computers and other school ICT equipment/devices is limited to educational purposes appropriate to the school environment.

2.2. The school has the right to monitor, access, and review all the use detailed in 2.1. This includes all emails sent and received on the school’s computers and/or network facilities, either during or outside school hours.

2.3. The use of any privately-owned ICT equipment/devices on the school site, or at any school related activity, must be appropriate to the school environment. Such equipment/devices could include a laptop, desktop, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular

device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate should check with their teacher.

2.4. When using the internet, it may not always be possible for the school to filter or screen all material. However the school will attempt to filter as much dangerous, illegal or inappropriate content as is possible.

However, the expectation is that each individual will make responsible use of such systems.

3. Monitoring by the school

3.1. The school has the capacity to monitor traffic and material sent and received using the school's ICT infrastructures. From time to time this may be examined and analysed to help maintain a safe school environment.

3.2. The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

However, as in 2.4., the expectation is that each individual will be responsible when using ICT.

SECTION A- INTERNET SAFETY AT SCHOOL

- INTERNET SAFETY RULES FOR PUPILS -

Note for Parents:

The sections below are designed to provide a guide to the rules covered by this Use Agreement, and to help you discuss the rules with your child. Teachers will also go over this section with pupils.

1. I must have a Use Agreement signed by me and by my parent before I am allowed to use the school ICT equipment.

All pupils, regardless of age or ability, must have a Use Agreement signed by their parent and those in Year 4 and above must sign their use agreements along with their parents. Use Agreements are becoming accepted as an essential part of ICT safety policy within programmes for schools and other organisations, including businesses.

2. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

This helps children and young people to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and pupil to work through an issue and so avoid the pupil making an unwise decision which could lead to serious consequences. Young children need ongoing guidance to help them become safe and responsible users of ICT.

3. I will follow the internet safety rules, and will not join in if others are being irresponsible.

Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major

problem. Often children become involved in these acts through peer pressure without thinking of the consequences.

4. I will not use the internet, mobile phones or any other ICT equipment at anytime to be mean, rude, offensive, or to harass any members of the school community like pupils and staff, while enrolled in the school.

The basic principles of politeness and respect extend to the use of ICT. If I come across inappropriate material I will not show it or share it with others.

5. If I accidentally come across mean, rude or dangerous material, I will tell the teacher straightaway, without showing any other pupils.

Because anyone at all can publish material on the internet, it does contain material which is inappropriate and in some cases illegal. The school has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a pupil may inadvertently stumble across something inappropriate. Encouraging pupils to tell a teacher immediately if they find something which they suspect may be inappropriate encourages critical thinking and helps children to take responsibility for their actions and keep themselves and others safe.

6. If I am not feeling safe at any time while using the ICT equipment, I will tell the teacher straight away.

Our school strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a child to feel unsafe could include: contact being made by a stranger through email or text message, the presence of 'scary' images on a computer screen, and/or misconduct by other pupils. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.

7. If I am sharing a computer with someone else, I share the responsibility for how it is used. If there is a problem, I will tell the teacher immediately.

Pupils often work together at a single computer. Any misuse of the computer can be traced back to whoever was logged on at the time. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.

8. I will check with the teacher or my parent before giving anyone information about myself or others when using the internet or a mobile phone – this includes home and email addresses and phone numbers.

This reduces the risk of your child, or other children being contacted by someone who wishes to upset or harm them or use their identity for purposes, which might compromise their privacy.

9. I will not be careless, try to damage, or steal any school ICT equipment.

10. I will not try to stop the network or any other equipment from working properly or change, delete other people's work without their permission. I will not try to change screensavers, desktop backgrounds, themes or hardware settings without the teacher's permission.

11. If I accidentally break something, or I find it broken when I start to use it, I will tell a teacher straightaway.

12. I will not print anything without the permission of the teacher.

13. I will not download any files such as music, videos, or programmes without the permission of the teacher, even if they are for schoolwork. If I am unsure, I will ask the teacher first.

Many files available on the internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses, or spyware. Some files may contain inappropriate or illegal material.

14. I must have a letter from home, requesting permission from school, before bringing any disk or other ICT device from home, unless it is part of my normal school equipment. If I am given permission, then I must use that ICT sensibly.

The devices referred to in this rule may include flash memory devices, iPods, MP3 players or mobile phones. Any pupils bringing such devices from home are asked to use them sensibly. This applies to the school site and any school-related activity.

15. I am aware the teacher can check any disk or ICT device (including all disks, memory storage devices, media players, cameras and mobile phones) I bring from home, before I use it with school equipment. I understand that viruses can be transferred to and from the school and accept there is no liability on behalf of the school should my personal or home equipment be compromised.

This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks or other storage devices such as USB sticks or memory cards. If your child is using a disk or other device to transfer work between home and school, it should be freshly formatted, or 'blank', before use. This may also stop any of your own personal material from finding its way onto the school's equipment. Even though every effort is made to keep school equipment virus-free, you should scan your child's disk or device for viruses before they use it again with your home computer.

16. I will not bring software or games from outside school to use on school equipment.

Installing software from home may cause conflicts with the software installed by the school. Our school must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software.

17. I will acknowledge where work has come from if I have copied it from somewhere.

The internet has allowed easy access to a huge range of information which can be incorporated into pupils' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. The value to pupils' learning is questionable if they have not thought through this information themselves.

18. Wherever I have a personal username, email address or login I will not share it with other people

It is very important that pupils learn the necessity of security awareness at an early age. Allowing others to gain access to their personal sites or information can leave themselves open to others misusing the internet in their name.

19. I will abide by the Mobile Phone Policy set out below and also not use or keep on my person mobile phones/SIM card devices during my time in school.

Making the most of these rules

You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children safe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend's house), or who they are with.

Mobiles Phones at School

Our school policy regarding mobile phones is that children should not bring them into school, however if for the purposes of travelling to and from school parents wish for their child to have a mobile phone on them then they are allowed to bring them to school but they are required to hand them into the school office before 9:00am, collecting them again at the end of the school day. Should parents wish to contact their child during the school day they may ring the office and we will arrange to get a message to the child or, in an urgent case, bring the child to the phone. Pupils are expected to restrict their use of mobiles on the school coaches solely for contacting parents.

SECTION B –SCHOOL COMPUTER USE AGREEMENT

To the Pupil and Parent:

- 1. Please read this page carefully as it includes information about your responsibilities under this agreement.*
- 2. Complete and sign the appropriate section.*
- 3. Detach and return this section to the school office.*
- 4. Keep **Section A** for your future reference.*

Our School will:

- do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the internet or school ICT equipment/devices at school or at school related activities.*
- work with pupils and their families to encourage and develop an understanding of the importance of internet safety through education designed to complement and support the Computer Use Agreement. This includes providing pupils with strategies to help keep themselves safe on the internet.*
- keep a copy of this signed use agreement form on file.*
- respond to any breaches in an appropriate manner.*
- welcome enquiries from parents or pupils about internet safety issues.*

Pupil's section

My responsibilities include:

- **I will read** this Computer Use Agreement document carefully with my parent.
- **I will follow** the internet safety rules and instructions whenever I use school ICT.
- **I will have no involvement** in use of ICT which could put me or other members of the school community at risk.
- **I will be respectful** of other pupils and staff when I use the internet outside of school.
- **I will take proper care** when using computers and other school ICT equipment.
- **I will keep** Section A of this document somewhere safe so I can read it again later.
- **I will ask** my teacher or my parents if I am not sure about something to do with this Agreement. I have read and understand my responsibilities and agree to follow the Computer Use Agreement. I know that if I breach this use agreement there may be serious consequences.

Name of pupil: **Class:**

Signature: **Date:**

Section for parent

My responsibilities include:

- **I will read** this Computer Use Agreement document and discuss the rules with my child
- **I will ensure** this Agreement is signed by me and my child and returned to the school.
- **I will support** the school's internet safety programme by encouraging my child to follow the internet safety rules and to always ask the teacher if they are unsure about any use of ICT
- **I will contact** the Headteacher or other staff to discuss any aspect of this Use Agreement which I might want to learn more about. I know I am welcome to do this at any time.

I have read this Computer Use Agreement and am aware of the school's initiatives to maintain a safe learning environment and the responsibilities involved.

Name of Parent:

Signature:

Date: