Crosshall Infant School Academy Trust

Computing Policies

Contents:

1. Introduction

"The government, local authorities and schools are encouraging the use of the internet to promote learning in a wide range of areas. Exploiting the online world is now a key means of extending and personalising the education experience of all learners. Young people hardly need to be persuaded to learn in this way.

Guidance to educational establishments on Child Protection and the use of the Internet, Cambridgeshire Education Child Protection Service and Education Computing Service (2007)

The framework provided by this document will help to create an environment where Computing technologies can be used for educational benefit whilst at the same time safeguarding members of the School's community from undesirable elements.

These policies apply to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school Computing systems, both in and out of school. A school online safety policy helps to ensure safe and appropriate use.

For the purpose of this document the term 'Crosshall Infant School' covers Crosshall Infant School Academy Trust, Nursery School and Kids Club.

2. Computing Curriculum Policy

Computing has become a life-skill and computer skills are vital in today's society. We believe that it is advisable for parents to consider the school's policy and strategies when allowing their children access to Computing resources at home.

Purpose of study

A high-quality computing education equips pupils to understand and change the world through logical thinking and creativity, including making links with mathematics, science, and design and technology. Computing equips pupils to use information technology to create programs, systems and a range of media and to understand the principles of information and computation, and how digital systems work. It also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

Aims

The national curriculum for computing aims to ensure that all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- are responsible, competent, confident and creative users of information and communication technology. The statutory curriculum requires pupils to learn:

Nursery and Reception

- This area has been removed from the curriculum in the new EYFS Framework September 2021. However, we are still ensuring that they children are being taught that a range of technology is used in places such as homes and schools. We are teaching them to select and use technology for particular purposes.

Key stage 1

- To understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions
- To create and debug simple programs
- To use logical reasoning to predict the behaviour of simple programs
- To use technology purposefully to create, organise, store, manipulate and retrieve digital content
- To use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet
- To recognise common uses of information technology beyond school.

Attainment targets

By the end of each key stage, pupils are expected to know, apply and understand the matters, skills and processes specified in the relevant programme of study.

2.1 The Vision of Computing at Crosshall Infant School Academy Trust

Computing is a tool to enable children to access and enhance their learning. We believe that through training our staff, and using appropriate equipment, we are able to provide excellent teaching. This therefore promotes children's learning and provides them with the skills they need to prepare them for the future.

2.2 Aims and Objectives for Computing:

- To provide a variety of computing experiences for all children.
- To ensure that specific materials, methods and opportunities are available for those children who need them.
- To ensure that Computing knowledge is developed at a level appropriate for each individual child.
- To ensure that Computing is embedded across all curriculum areas.
- To encourage children to be involved with a range of equipment and programs.

- To ensure that a range and balance of teaching and learning methods are employed.
- To embrace changes to the curriculum to ensure development in all areas of the curriculum

2.3 Curriculum Planning

- Planning is based on the KS1 National Curriculum.
- Curriculum planning is carried out in three phases, namely: long term - yearly; medium term – topics; short term – weekly.
- The SIMS management information system provides assessment tools to monitor pupil progress in all curriculum areas. KS1 also have an assessment sheet to track progress.
- To ensure every child has equal opportunities to use Computing and make progress
- An ICT focus group consisting of the Headteacher, Computing subject leaders, ICT administrator, the Finance Manager and representatives from each year group meet on a half termly basis to discuss changes to the curriculum, new software and hardware available, online safety issues and the development of Computing throughout the school.

2.4 Resources

Every classroom has:

- An interactive screen (that can run without a computer connected)
- A digital camera
- A teacher laptop
- Relevant and up to date software installed on teacher's laptop.
- Access to a varied range of IT equipment, e.g. Beebots, Digital Video Recorders, netbooks.

Computer Suite has:

- An interactive screen
- 15 laptops

Laptop Trolley has:

- 14 laptops

Nursery has:

- An interactive screen
- Digital Cameras
- A teacher's laptop
- Relevant and up to date software installed on teacher's laptop
- A CD player
- A YOTO device for independent story telling
- Access to netbooks, laptops, kindles, bee-bots, talking turtles and a programmable truck called Big Track.

Music Room has:

- An interactive LCD Screen

Printing and Photocopying Facilities:

- Two network printers, which are also colour photocopiers, are available for use in the Office and Reprographics Room
- A colour printer is also located in the Kids Club

Hall has:

- A screen and projector
- Surround sound
- Network, display and audio connection points for use during assemblies and other activities

Office has:

- 6 PCs for Office Staff use
- Franking Machine
- Photocopier \Network Printer
- Finance Printer

Staff Workroom has:

- 2 PCs

Kids Club has:

- 6 laptops
- Digital Table
- 1 Office PC
- 1 printer

2.5 Roles and Responsibilities

Headteacher:

- To ensure consistent implementation of the Computing policy
- To manage the Computing budget
- To be aware of Health and Safety Policy and links to Computing usage
- To manage the school improvement plan for Computing
- To ensure online safety guidelines adhered to

Computing Subject Leader

- To advise colleagues on planning and software
- To identify training needs and support
- To ensure Computing progression
- To create a school portfolio of evidence
- To research new equipment, software and solutions
- To ensure that all online safety information is up to date and distributed to staff

ICT Administrator

- To liaise with external agency to support technology within school
- To be the point of communication for staff regarding any technical problems
- To manage website and all associated external companies who provide web based products

External Computing Support agency – idash.

- To manage school network
- To implement and maintain most ICT equipment
- To implement new equipment, software and solutions
- Appendix G provides detailed information about IT security that was emailed to all staff
- To dispose of redundant/broken equipment in accordance with health and safety guidelines.
- To ensure that the school's IT infrastructure is secure and is not open to misuse or malicious attack

- To manage anti-virus system and firewall system
- To monitor e-mail and internet usage when required

All Staff

- To adhere to the guidance within this document and associated Computing policies and to ensure confidential information, such as usernames and passwords remain confidential.

3. Internet and Acceptable Use Policy

3.1 Internet Provision, Firewall and Virus Protection

- Internet Provision supplied by BT
- Watchguard Firewall, which blocks, and regulates web content, is managed by i-dash
- AVG antivirus is present on all workstations. All users are to ensure that they connect to the network, when in school, to ensure all anti-virus systems are updated.
- Spam is blocked using the integrated spam filters in Office 365, as provided by Microsoft.

3.2 School Website and Third Party Providers.

School Website

- The school website is provided by' Primarysite'. All day to day administration is managed by the ICT administrator
- There are various legal requirements to display information on our website. These are detailed in Appendix D
- Staff and Governors have access to a secure area of the website. Access is controlled by the ICT administrator

Third Party Provision

- Online payment provision is supplied by WisePay. Parents and staff use the link from our website to make payments for dinner money, educational trips and Kids Club fees. WisePay ensure confidentiality and also a secure payment area. Email and text messages can also be sent to parents using this system.
- Netmedia provide the system to make parents evening booking appointments.
- Gilt Edge provides a secure online uniform ordering system.
- MailChimp provide a means to e-mail information to our parents. This is managed by the school office
- Remote access to the school network is provided through the WatchGuard VPN facility. Remote access is provided on an individual basis by idash.
- Capita provide the MIS system, Sims. This contains all data relating to our pupils and staff. The Sims system is hosted locally on a Hyper-V server, residing on the PDC, and is accessible via the local network and school VPN facilities. The Sims system is managed by the ICT administrator and access is granted by means of a secure logon and password.
- Microlibrarian Systems provide the software which allows the use of a managed library system
- Sage is the accounting software used by the finance office and Kids Club

3.3 Acceptable use of the Internet

Please also refer to Section 4, Online safety, to complement this section of this policy.
The use of the internet is now an integral part of most people's daily life. Whilst this brings untold benefits there are also associated risks. There are many concerns regarding internet safety and, here at Crosshall Infant School, we are very keen to ensure that our children are aware of the potential dangers and know what to do and who to talk to if they have any concerns. We discuss key issues with the children, whilst bearing in mind their young age. Obviously, we need to stress the importance of being safe but we have no wish to scare the children or to stop them enjoying using the internet safely.

To do this we:

- Ensure all access to the internet in a school setting is supervised.
- Publish guidance for parents on our school website, through emails and display an online safety PowerPoint at different events throughout the year.
- Ensure all staff are aware of what is "acceptable use" and who they should contact if they have any worries or concerns regarding the inappropriate use of ICT.
- Ensure children are aware that they can talk to a member of staff if they are unsure about any aspect of internet use.
- Display online safety posters containing key points to keep the children safe, throughout the school.
- Have the ability to monitor all internet traffic and review which sites have been accessed.

3.4 E-Mail Provision and Use

- All members of teaching staff, office staff and all support staff have been allocated a school e-mail address. Users may make use of the school e-mail system for personal use on the condition that it does not interfere with their work and all content is deemed appropriate for a primary school setting. All users are warned that the school network is subject to monitoring and all e-mail content may be examined.
- Any member of staff who receives an e-mail which they believe may be from a malicious sender or contain inappropriate material should contact the ICT administrator and refrain from opening the e-mail and / or any attachments. Should such items be opened inadvertently, the ICT administrator should be notified immediately and the device should be disconnected from the network. The email and any attachments should be provided to the ICT administrator.
- All emails should be written with care and consideration, as if they were on school headed paper, representing Crosshall Infant School Academy Trust. E-mail is regarded as 'Public Property', as any message may be forwarded.

3.5 Copyright

- Respect for copyright and the correct usage of published material needs to be taught and adhered to by staff.

- Schools are allowed limited use of copyright works without the permission of the copyright owner. These are detailed by the UK Patent Office and can be found at www.ipo.gov.uk.

3.6 Mobile Phones

- Mobile phones should not be used within settings by staff or parents. Parents are asked to refrain from using mobile phones whilst collecting and dropping off their children at both Day Care and Nursery.
- All adults in school are aware that mobile phones should not be used in the presence of children, unless in an emergency or exceptional circumstances, e.g. on a school educational visit to advise of return times.
- Staff members are not allowed to use their personal home or mobile phones to contact children under any circumstances.
- Staff members must not be in direct contact with pupils via any social media sites

4. Online Safety Policy

We teach our children to use the internet safely and responsibly. We also ensure that all pupil access to the internet, when in school, is supervised.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely, is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put children at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the 'off-line' world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate these completely. It is therefore essential, through good educational provision, to build pupils' awareness and resilience to the risks to which they may be exposed, in order that they have the knowledge to recognise such a threat and are confident that they know who to approach for help and / or advice.
The school network is protected by a Unified Threat Management (UTM) solution provided by WatchGuard, which filters inappropriate content. This is managed in house and, whilst the majority of broad filters can restrict access to various websites, individual blocks can also be applied should any internet site be deemed to be inappropriate for our setting. We also publish guidance on our website, in the form of an online safety brochure for parents. This brochure is detailed as Appendix C.

A government review has also taken place and the findings are detailed within the 'Byron Review'. A website link to this document is detailed in Appendix C, along with web links to Ofsted guidance notes relating to internet safety.

Training regarding online safety is also undertaken by staff and parents are contacted to ascertain if online safety training is required. At all presentations where parents are involved, e.g. Reading Workshop, Maths Evening, the PowerPoint presentation regarding online safety is played, in an attempt to 'drip feed' as much online safety information as we can to parents. The link to this presentation is detailed with Appendix C.

We have adopted a whole school approach to online safety with the teaching and use of an online safety poster. The poster outlines key messages to keep the children safe when using technology and is displayed throughout the school. It has also been shared with parents via email. The poster is supported by regular lessons on online safety planned into the curriculum as the children progress through the school.

Responding to Incidents –
It is important that all members of staff are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology. If an online safety incident occurs, document the event using the designated blue form and refer immediately to the designated members of staff for child protection.

5. Social Media and Social Networking

5.1 Social Media Sites

'Social media' and 'Social networking' refer to web sites that people use to share information, ideas and images. Such sites include, Facebook, Twitter, YouTube. If staff or members of the Crosshall Infant School community use any social networking sites for their own personal use,

they are advised to ensure that their individual security settings are at the most secure level when using any social media sites to ensure maximum privacy and security.

5.2 Staff Acceptable use

Members of staff who use social media sites for their own personal use need to be aware that any comments or images posted on-line adhere to the following guidelines:

- Do not bring the school into disrepute
- Do not bring the teacher into disrepute
- Do not expose the school to legal liability
- Reflect safe internet practices
- Reflect the school's standard of behavior and staff code of conduct

Disciplinary procedures may be invoked if **any** member of staff is viewed as bringing the school into disrepute by disregarding the above guidelines. Should any member of staff inadvertently access or receive unsuitable material this must be brought to the attention of the ICT administrator in the first instance, who will liaise with the Computing leader and / or the Headteacher where appropriate.

Guidance re use of Facebook and also Social Media Guidance, is available. Various web links are detailed in Appendices A and B.

5.3 Misuse by Parents or Non Staff members

Parents also use social media websites and problems have been encountered when detrimental or adverse comments are made about the school and /or members of staff. Should any such comments be brought to the attention of any members of staff, they should be referred to the Headteacher who will decide upon the appropriate course of action.

6. Use of Images Policy

The use of images can be divided into three broad categories:

- Images taken by Academy Trust staff for education and publicity purposes.
- Images taken by parents at school events.
- Images taken by third parties.

6.1 Images taken by staff of the Academy Trust

On 25 May 2018 most processing of personal data by organisations will have to comply with the General Data Protection Regulation. (See appendix) An image of a child is personal data and it is, therefore, a requirement that consent is obtained from the parent of a child for any images made such as those used for school web sites, productions or other purposes.

Written consent is obtained from the child's parent/carer via all Admission Forms, and kept in the child's file, covering all cases where images of children are to be used. Parents may withdraw consent at any stage, but would need to do so in writing.

We take extra care in relation to particularly vulnerable children such as those who are in public care, recently adopted, or those resettled following on from domestic violence.

6.2 Parents wishing to take images at school events

The Data Protection Act does not prevent parents from taking images at school events, but these must be **for their own personal use**. Any other use would require the consent of the parents of other children in the image.

The Headteacher, in consultation with Governors, will agree when parents are to be permitted to take images. This information will be included in invitation letters to parents, usually taking place as a special photo call session at the end of an event – this avoids distraction and disturbance and also allows for the withdrawal of any children whose parents/carers have not consented.

It is recommended that wherever possible the school should take our own 'official' photos or videos in order to retain control over the images produced.

6.3 Publishing or displaying photographs or other images of children

The DfE advise the following:

- If the pupil is named, avoid using the photograph.
- If the photograph is used, avoid naming the pupil.

Whatever the purpose of displaying or publishing images of children, care should always be taken to avoid the possibility that people outside the school could identify and then attempt to contact pupils directly.

If a child is photographed by a newspaper, the photo becomes the property of the newspaper and the newspaper has the final say as to how it is used. (N.B. images can be placed by editors on the newspaper's website). Generally, newspaper photos of groups of 12+ children do not have the names of the children attached. However, photos of groups of less than 12 children are likely to include the full name of the child in the accompanying caption. Parents need to be aware when they give consent that this is the position.

7. Staff Laptop Use Agreement and Staff Awareness and Acceptable Use Agreement

All teaching staff, some support staff and some teaching assistants, are provided with a laptop by the school. The user agreement is detailed as Appendix E
All staff are expected to be aware of various issues with regard to online safety, Health and Safety and Social Media use. The agreement is detailed as Appendix F.

Approved: January 2025 **Next Review Due: January 2026**

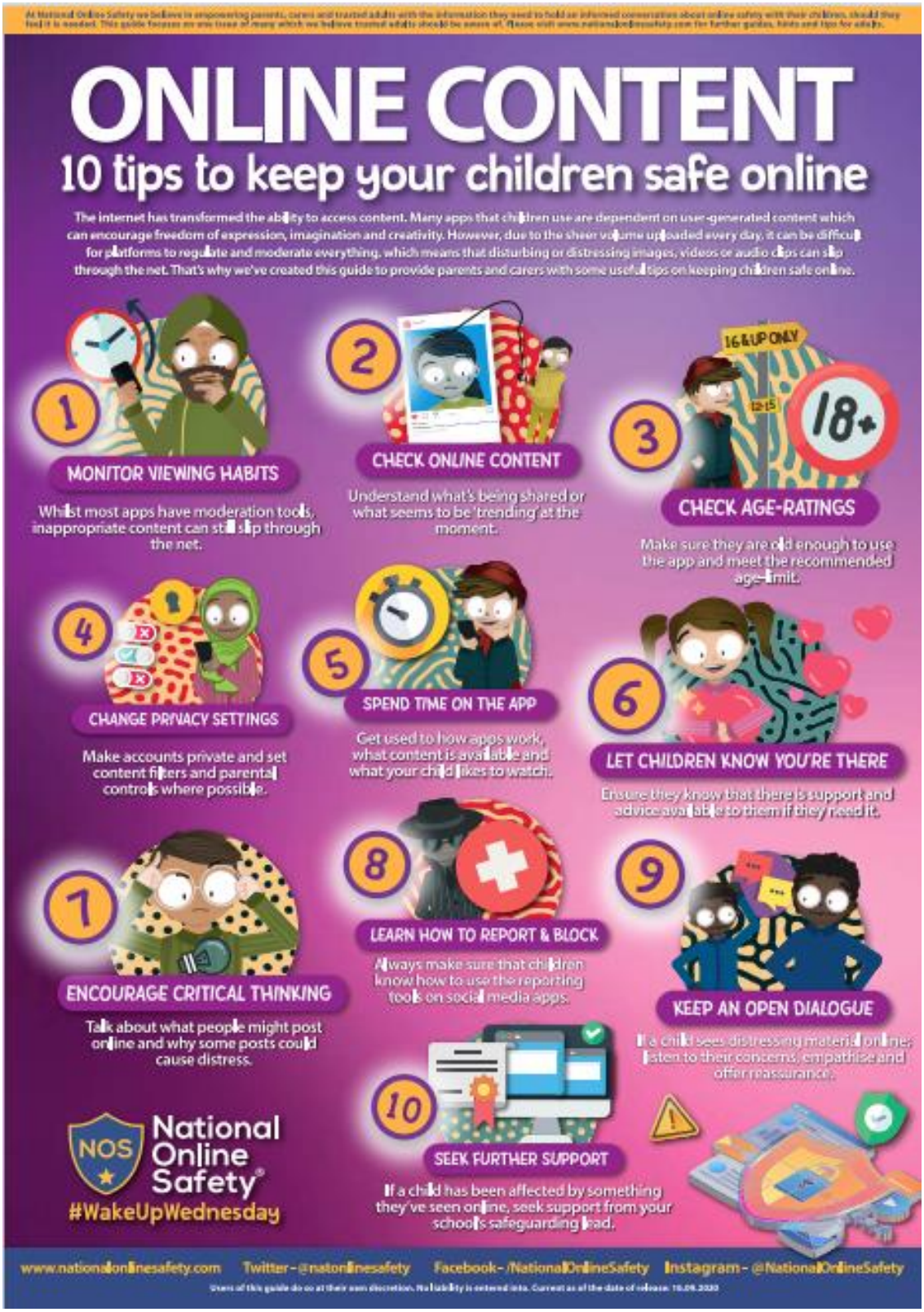
Appendix A: Social Media Guidance

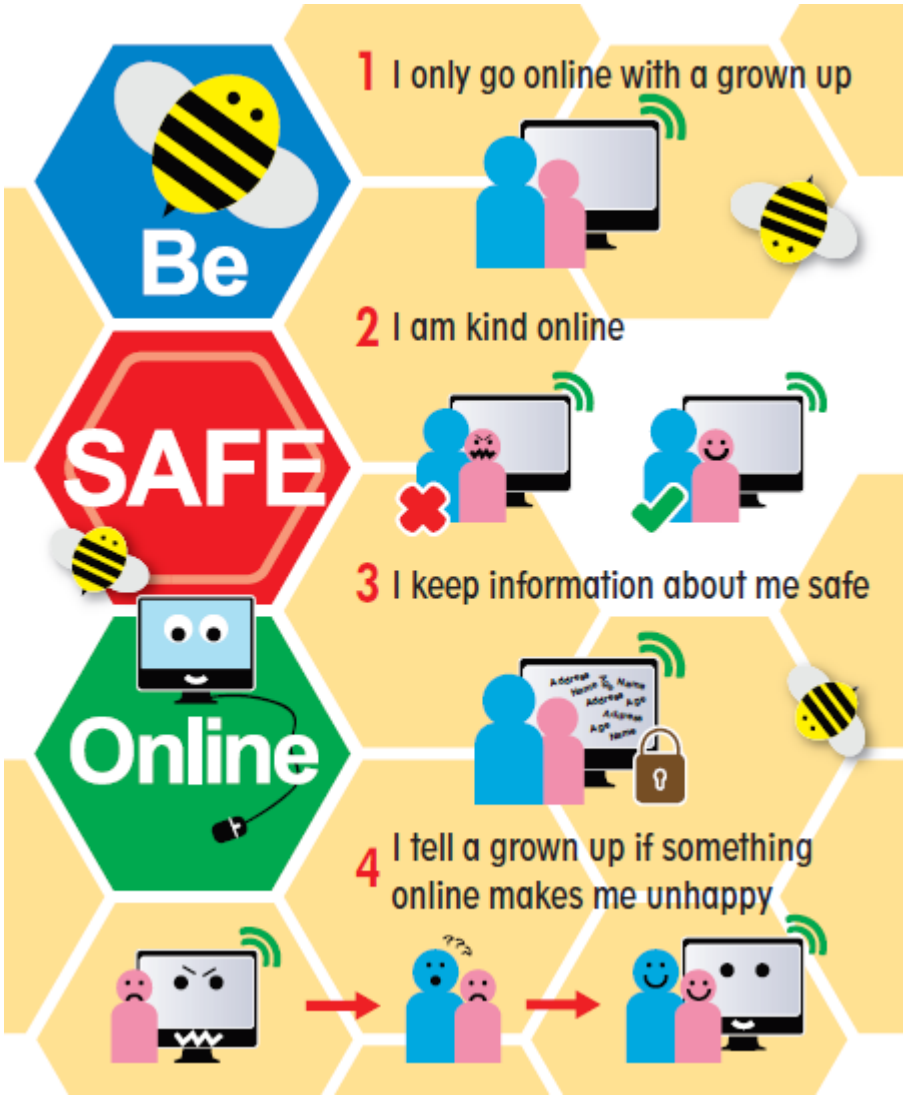
Further information is available from the following web sites:
http://www.childnet.com/
https://khub.net/learntogether https://www.nasuwt.org.uk/article-listing/using-social-media-safely.html http://www.gtcs.org.uk/web/FILES/teacher-regulation/professional-guidance-ecomms-social-media.pdf

Appendix B: Facebook Guidance for Staff

Further information is available from the following web sites to provide teachers and all school staff with guidance regarding the use of Facebook.
http://www.hull.nasuwt.org.uk/Facebook%20Guide.pdf
http://www.edudemic.com/every-teachers-must-have-guide-to-facebook/

Appendix C: Online safety Supplementary Information





Website Link to our Power Point Presentation

https://primarysite-prod.s3.amazonaws.com/uploads/d2e0b933d1ec44aebe5aaef22db70ea3/66e1/esafetypresentation.pdf

Website Link to Byron Review

http://media.education.gov.uk/assets/files/pdf/s/summary%20of%20the%202008%20byron%20review%20for%20children%20and%20young%20people.pdf

Website links to Ofsted Online safety Guidance

https://www.gov.uk/government/publications/advice-on-child-internet-safety-10-universal-guidelines-for-providers
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/177099/DFE-00004-2012.pdf

Appendix D: School Website – Necessary Information to Meet Legal and Ofsted Requirements. see https://www.gov.uk/guidance/what-maintained-schools-must-publish-online#history

The following subheadings relate to the legal requirements for information which must be available on our website:

- **Pupil premium allocation, use and impact on attainment**

Document Name	Author Responsibility	Legally Required
Prospectus	Headteacher	Yes

- **Curriculum provision, content and approach, by year and by subject**

Document Name	Author Responsibility	Legally Required
Curriculum Overview Guidance Booklet for parents	Assistant Headteachers	Yes
Curriculum Focus	R, Y1 and Y2 team leaders	Yes
Prospectus	Headteacher	Yes

- **Admission arrangements**

Document Name	Author Responsibility	Legally Required
Admission Policy	Headteacher	Yes
Cambridgeshire Admission Appeals Information and Timetable	Local Authority	Yes

- **The school's policy in relation to behaviour, charging and special educational needs (SEN) and disability provision.**

Document Name	Author Responsibility	Legally Required
Behaviour Policy	Headteacher	Yes
Charging and Remission Policy*	Headteacher	Yes
Letting Policy	Headteacher	Yes
Equality and Diversity Policy	Headteacher	Yes
Prospectus	Headteacher	Yes

- **Links to Ofsted Reports and DFE achievement and attainment performance data.**

Document Name	Author Responsibility	Legally Required
Ofsted Report	ICT administrator	Yes
Raise online reports and County data	ICT administrator	Yes
CIS Data Dashboard	Ofsted	Yes
Assessment Results	ICT administrator	Yes

- **The name, postal address and telephone number of the school and the name of a person to whom enquiries should be addressed.**

Document Name	Author Responsibility	Legally Required
Contact Page on Website	ICT administrator	Yes
Request for Paper Copies	ICT administrator	Yes

- **The report prepared by the school under Section317(5) (a) of EA 1996 duties of governing bodies in relation to special education needs.(c)**

Document Name	Author Responsibility	Legally Required
Special Needs Policy	Headteacher	Yes

- **The school's charging and remissions policy**

Document Name	Author Responsibility	Legally Required
Charging and Remission Policy	Headteacher	Yes

- **The school's complaints procedure**

Document Name	Author Responsibility	Legally Required
Complaints Policy	Headteacher	Yes

- **PE and Sports Premium**

Document Name	Author Responsibility	Legally Required
PE and Sports Premium	Headteacher	Yes

- **Governor's information and duties**

Document Name	Author Responsibility	Legally Required
Governors Information and Duties	ICT administrator	Yes

- **A statement of the school's ethos and values. Governing Bodies can decide if they wish to publish additional information for parents.**

Document Name	Author Responsibility	Legally Required
Mission Statement (Pencil's)	ICT administrator	Yes
Logo	ICT administrator	Yes
Prospectus	Headteacher	Yes
Golden Rules	Headteacher	Yes

Other documentation available on the website

The following table is a list of all other documents which are detailed on the website and which need to be up to date.

Document Name	Website Location	Author Responsibility	Legally Required
Nursery Ofsted Report	Nursery, Ofsted	ICT administrator	Yes
Nursery Prospectus	Nursery, Admissions	Admissions Secretary	Yes
Nursery Change of Contact details	Nursery, Forms	Nursery Leader	No
Nursery Pre-Admission	Nursery, Admissions	Admissions Secretary	No

Nursery Sickness and Medical	Nursery, Forms	Nursery Leader	No
Keywords and Reading Guide	Key Information, Learning Resources	Reception Team Leader	No
Teaching Maths	Key Information, Learning Resources	Maths Subject Leader	No
Change of Contact Details	School, Forms	School Office Administrator	No
Guidance on Infection Control	School, Forms	PA to Headteacher	No
Sickness and Medical	School, Forms	School Office Administrator	No
Home School Agreement	Key Information, Policies, School Policies	School Office Administrator	No
Anti Bullying Policy	Key Information, Policies, School Policies	Headteacher	Yes
Equality Act Objective Policy	Key Information, Additional Information	Headteacher	Yes
ICT Mark	School, Key Information	Computing Subject Leader	No
Protocol for Children not Collected	Key Information, Policies, School Policies	Headteacher	Yes
Publication Scheme	Key Information, Policies, School Policies	Headteacher	Yes
Articles of Association	Key Information, Additional Information	Headteacher	Yes
Academy Funding Information	Key Information, Additional Information	Headteacher	Yes
Menus	School, School Lunch	Kitchen Manager	No
Curriculum Focus	Key Information, Additional Information, Curriculum Information	R Y1 & 2 Team Leaders	Yes
Last approved governor meeting minutes	Governor Area	ICT administrator / Governance Professional	
Complaints Procedure	Key Information, Policies, School Policies	Headteacher	Yes
Online safety information	Key Information, Additional Information	NSPCC / Computing Subject Leader	No

Web Links

Name	Website Location	Author Responsibility
School Profile http://schoolsfinder.direct.gov.uk/8735203/overview/?d=1&sbtSearchSchools=Search&searchString=PE19+7GG&PC=PE19%207GG&pagetype=search-results	School Key Information	ICT administrator
Cambridgeshire County Council http://www.cambridgeshire.gov.uk/childrenandfamilies/education/	Key Information, Policies, School Policies	ICT administrator
Department for Education http://www.education.gov.uk/	Key Information, Additional Information	ICT administrator
General Data Protection Regulations https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/	Key Information, Policies, School Policies	
Free School Meals https://forms.cambridgeshire.gov.uk/customer/servlet/ep.app?ut=X&type=253860	School Lunch	Finance Assistant

Appendix E: Staff Laptop Agreement

Management

This laptop is owned and managed by Crosshall Infant School. The school is responsible for insurance, but it would be prudent for the named user to advise their own insurance company of the existence of the equipment.

The Laptop specified below is on long-term loan to: (Staff Name)

Laptop Details: (Make Model and serial number of computer)

Start of loan date: End of loan date:

- The laptop is to be returned to school upon the request of the Headteacher or ICT administrator
- The laptop may be checked for correct use at any time by the Headteacher or ICT administrator

Terms and Conditions – Equipment Loan

1. During your loan period, the laptop remains the sole property of Crosshall Infant School Academy Trust and should be treated as such.
2. Crosshall Infant School reserves the right to re-call laptops from users at the Headteacher's and/or ICT administrator's discretion.
3. Your use of the laptop will fully comply with the acceptable use conditions detailed within the Computing policy document.
4. General services and repairs must be carried out by or authorised by the ICT administrator. **Third parties must NOT have access to the laptop unless authorised by the ICT administrator**. Third parties include, partners, family members and friends.
5. **Accidental damage both inside and outside the Academy will be managed as follows:**
   a) **The cost of the first incident of any accidental loss or damage of the laptop will be met by the Academy.**
   b) **All subsequent incidents the insurance excess of £250 will be met by the user of the laptop.**
6. Insurance of the laptop. The laptop is fully covered by Crosshall Infant School Academy Trusts' insurance, subject to terms and conditions. You are not required to ensure the laptop is covered by insurance at all times, however you may be asked to reimburse the Academy for equipment that is lost, damaged or stolen if a previous such event has occurred. Each case will be looked at on an individual basis.
7. The system has been loaded with an up to date anti- virus software package (AVG). The named user is to ensure that the software is kept up to date. The laptop must be brought into school each day to update the anti- virus software. (If part time member of staff, then the laptop must be brought in each day you are working in school.)
8. Ensure your individual logon and password is confidential.
9. Confidential data must never be stored on memory sticks or such devices.
10. The laptop must always be packed in its carry case when being transported and care must be taken when transporting between school and home that the laptop is secure and out of sight.

Declaration:

I certify that I have read, understood and agree to comply with the above instructions.

Signed: Date:

Appendix F: All Staff Awareness and Responsible Use Agreement

This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its content. Any concerns or clarification should be discussed with the ICT administrator.

- I will only use the Academy's e-mail/Internet/Website and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will comply with Crosshall Infant Schools system security and not disclose any passwords provided to me by the Academy or any other related authorities.
- I may make use of the school email system for personal use on the condition that it does not interfere with my work and all content is deemed appropriate for a primary school setting.
- I will not install any hardware or software without permission from the network manager. Home printers and home internet access are automatically approved.
- Images of pupils will only be taken, stored and used for professional purposes in line with the Crosshall Infant School's policy and with written consent of the parent or carer.
- I confirm that, in the event that I notice inappropriate use of social networks, school computers or use of the internet by staff, pupils or parents, I am aware of the correct procedure to escalate these concerns.
- I will ensure my online activity, both personal and when at school, specifically using any social media websites, will not bring my professional role, nor Crosshall Infant School into any disrepute.
- I will support and promote Crosshall Infant School online safety guidelines.
- I will not place any confidential information, relating to pupils, staff or Crosshall Infant School on memory sticks or other such devices.
- I understand that my use of the school Internet and school e-mail can be monitored and logged.

Signed:

Name:

Date:

APPENDIX G: Information from idash regarding IT Security

An IT meeting was held in July 2017 with Idash who are currently covering all IT /security issues for us. As a result, the following items are to be implemented with immediate effect, without exception:

No USB memory sticks are to be used at all, anywhere within school. Any transfer of information is to be saved to the General drive and then transferred to specific place as required.

All teachers and line managers have been allocated a personal laptop and this is to be used for all school work. Nothing should be downloaded/transferred to personal laptops or computers. A lot of money has been invested in the provision of IT for relevant staff and we need to ensure that we are using it correctly and securely.

No one should be using a personal email for any school work. Everyone has been allocated a school email address and this is how information must be shared. Email is a key form of communication within school and all staff should be accessing their school emails at least once a day to ensure they are abreast of all school information. If anyone has a problem with their email account please speak to me as a matter of urgency.

Idash are to set up personal folders on the General drive for all teachers as a place where information can be saved. It is important that this facility be used for saving work rather than individual desktops as if there is ever a problem with your laptop, information/work can be lost. However, if it is saved to the General drive, this is via the server and can be retrieved.

All teachers/line managers should have VPN access on their laptops to ensure they can work on the server outside of school.

Please do not open any files attached to emails that you are not expecting, especially Word or Excel documents. You need to be sure that they are coming from a recognised source. If you are unsure then please check with the office and we can arrange for it to be quarantined.

Please do not use 'Dropbox' to share confidential school information as it is not secure enough. Information that you wish to share should be via the General drive and a relevant link added to an email.

Finally, all staff have signed an IT Agreement as part of their contract and/or appraisal process, in which the above items are covered. Any deviation from this would be considered a breach of the agreement

APPENDIX H. Cyber Security in School. Information for Staff and Governors

1. **What is cyber security and why it matters to Crosshall Infant School**

Cyber security is about protecting the **devices** we use, and the **services** we access online from theft or damage. It is also about preventing unauthorised **access** to the vast amounts of personal data we store on these devices and in online accounts.

A cyber security incident can affect the school's ability to function, the security of its data and its reputation. We already follow similar approaches to manage risks and responsibilities around GDPR and pupil safeguarding.

2. **Roles and responsibilities of the Governing Body**

The role of governing boards is strategic and focused on ensuring that the school has IT policies and procedures in place that cover the use of ICT systems and data security, including compliance with GDPR.

The following processes and procedures have been put in place to **seek out information**, **raise awareness**, and **improve preparedness** in case of an incident.

3. **Provision of IT Services:**
   - We currently employ the services of i-dash Limited to provide integrated technology solutions to our IT needs, both present day and forecasting future requirements.
     - They have an in house Software Development Team who we can call on for application solutions meeting our needs and facilitating change and growth.
   - This service is deployed in house via the School Administration Team
   - I-dash have been fully consulted and are regularly consulted about security and the safety of our digital service.
     - WatchGuard and Bitdefender are installed and monitored in line with every element of our digital service
   - We have a full backup process and restoration process in place and this is covered within the Critical Risk Management Plan

4. **Awareness:**

All staff, regardless of role are required to familiarise themselves with the ICT awareness and responsible use policy and sign to say they will comply with the requirements of that policy at all times. This document covers use of equipment, systems and security awareness.

- Cyber security training is also undertaken by staff on a regular basis and all updates disseminated accordingly.
- School policies reflect the importance of good cyber security
- If any incidents are recorded, this information would be circulated to all staff and a full enquiry undertaken with i-dash

5. **Being Prepared:**

Being prepared for the potential impact of a cyber security incident is crucial in helping the school minimise disruption should an incident occur. The Critical Incident Plan covers any major disaster but day to day control would be via i-dash who control our digital network off site.

- Hard copy of all stake holder's data is available in the event of a temporary loss of internet connection, enabling the school to operate.
- The telephone system is designed to enable access should the school's network be temporarily unavailable. School mobile phones are also available in an emergency, held by the Headteacher and Site Manager.
- All cashless payments are via WisePay enabling parents to continue to make payments.

6. **Immediate action to take if the school becomes a victim of a cyber incident:**

The school's Critical Incident Management Plan lists the key external IT provider who would take on the management and control of the incident, together with the reporting to the Action Fraud.

The Information Commissioner's Office (ICO) would also need to be informed and the school would call on the Data Protection Officer, via County ICT Services – Paul Stratford to undertake this task. This is co-ordinated via the school's in house admin team and ensures full compliance with GDPR.

APPENDIX I

Crosshall Infant School Academy Trust - Remote Learning Protocol

March 2021

Introduction

This protocol aims to ensure that live lessons with pupils at home, are safe, secure and continue to model the high standards set by our school with our children.

This is guidance for running live lessons over Zoom or providing individual support to pupils via Zoom or telephone and how to do this safely and best engage the children.

Principles of live teaching

- Adhere to the school's staff and pupil behaviour policy (code of conduct) – professional attire, language etc. Treat a live virtual classroom just as you would at school
- Turn your camera on and have your camera at eye level
- Stay muted unless you're talking to reduce background noise
- Make sure you sit in a well-lit room, ideally not a bedroom
- Be mindful of what's going on behind you. Think about having a solid wall behind you, not a mirror or turn on a virtual background
- Do not post pictures of your virtual class on social media or elsewhere online
- If contacting a child via phone from home, please block your number using 141. Agree times with the parent when you are intending to call.

Parental consent –Zoom accounts should only be accessed by people over the age of 18. Children taking part in Zoom calls must access via a parent/carers account. The name on the account should allow the staff member who is hosting the meeting to easily identify who is joining the call.

- The title of Zoom meetings will be scheduled with the lesson and year group
- We will share the link to meetings with parents/carers in advance via email.
- The host will start the meeting promptly at the agreed time. The host will monitor the waiting room and admit children after the start of the meeting as long as the name on their account allows the host to easily identify who is in the waiting room.
- The host will always have control over the screen sharing facility
- The Waiting Room feature must be used to protect our Zoom virtual classroom and keep out those who aren't supposed to be there.
- Children will be reminded not to use the chat facility.
- If someone who's not meant to be there somehow manages to join our virtual classroom, we can easily remove them from the participant's menu.

The following safeguarding measures are in place:

- The Zoom meeting is password-protected: We will create a password and share with our pupils via school email or our school platform so only those intended to join can access a virtual classroom.
- 'Join before host' is disabled: Pupils cannot join class before the teacher joins and will see a pop-up that says, "The meeting is waiting for the host to join".
- The host member of staff should be the last to leave the meeting. The host must always exit the live meeting **for all** at the end.
- Use a random meeting ID - It's best practice to generate a random meeting ID for each session, so it can't be shared multiple times. This is a recommended alternative to using our own Personal Meeting ID, which is not advised because it is essentially an ongoing meeting that's always running.
- Hosts will disable participant annotation in the screen sharing controls to prevent pupils from annotating on a shared screen. This can only be done when you are sharing your screen. Click the security button and then untick the 'annotate shared content' option.

Additionally, teachers have a couple of in-meeting options to control your virtual classroom:

- Disable video: Turn off a student's video to block distracting content or inappropriate gestures while class is in session.
- Mute pupils: Mute/unmute individual pupils or all of them at once. Meetings can be set up with the Mute Upon Entry facility in place.
- Attendee on-hold: An alternative to removing a user, you can momentarily disable their audio/video connections. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate.
- Pupils will be reminded not to share personal information during the session.
- Security Icon in Toolbar: Visible only to hosts and co-hosts of Zoom Meetings, the Security button provides easy access to several existing Zoom security features, as well as a new option to turn on the Waiting Room in-meeting. This button allows us to remove participants, lock the meeting, and decide if we want to allow our participants to screen share, chat, rename themselves, and annotate on shared content.

First and ongoing virtual lessons

- Spend some time at the beginning checking that children understand their audio and video.
- Discuss online etiquette and expectations of the children in their first virtual class and periodically revisit this topic.
- Take time to promote questions, comments, and reactions from the class. Show children how muting and unmuting works and support with asking questions or sharing comments aloud.

  Most importantly, we are aiming to have fun with this new technology and engage in social interaction virtually.