St Nicholas
C of E Primary School

Online Safety Policy

Online Safety Co-ordinator: Anita Hartley
Executive Headteacher: Adam Walsh
Online Safety Governor: Caroline Harris

Adopted: December 2019 **Revised: December 2020**

1. Introduction

At St. Nicholas C of E Primary School we understand the responsibility we have to educate our pupils on online safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

St. Nicholas C of E Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive online safety programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the governors.

For expectations regarding the taking, distribution and publication of photography and videos at St. Nicholas C of E see the Phones and Camera Policy.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy, Code of Conduct policy, Mobile Phone Policy, Photography and Video Policy, and Equal Opportunities Policy.

2. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in St. Nicholas C of E Primary School. All staff on the Child Protection team have received Warwickshire's Safeguarding training.

Karen O'Shea is the designated safeguarding lead, Laura Newell is the deputy safe guarding lead, Sue Godson, Hannah Lowerson, Sally Long, Nick Harwood and Anita Hartley are all also trained as designated safeguarding leads. Adam Walsh, Executive Headteacher, has overall responsibility.

It is the role of these staff members to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection), and Childnet. The Executive Headteacher ensures Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school online safety procedures.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the internet

- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website and social media.
- procedures in the event of misuse of technology by any member of the school community
- their role in providing online safety education for pupils.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school.

Managing the school online safety messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The online safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- Online safety posters will be prominently displayed.

3. Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote online safety.

- We provide opportunities within a range of curriculum areas to teach about online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the Computing curriculum.
- Pupils are aware of the impact of online bullying through PSHE and Online Safety lessons and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

4. Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

The school maintains and supports the managed filtering service by Warwickshire ICTDS. Any filtering issues should be reported immediately to ICTDS via the Online Safety Co-ordinator or the Executive Headteacher. Any changes to filtering must be authorised by a member of the senior leadership team. The school infrastructure and individual workstations are protected by up to date anti-virus software.

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

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the Online Safety Co-ordinator and an email sent to ICTDS so that they can block the site.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the School currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		✔					✔	
Use of mobile phones in lessons			✔					✔
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones / cameras				✔				✔
Use of other mobile devices eg tablets, gaming devices		✔					✔	
Use of personal email addresses in school, or on school network				✔				✔
Use of school email for personal emails				✔				✔
Use of messaging apps		✔						✔
Use of social media		✔						✔
Use of blogs		✔					✔	

When using communication technologies the School considers the following as good practice:

- The official Welearn365 email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the Welearn365 email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person - in accordance with the School's policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used in the Early Years and KS1, while pupils at KS2 and above will be provided with individual Welearn365 email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

UNSUITABLE OR INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✔
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✔
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✔
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✔
Pornography				✔	
Promotion of any kind of discrimination				✔	
Threatening behaviour, including promotion of physical violence or mental harm				✔	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✔	
Using school systems to run a private business				✔	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				✔	
Infringing copyright				✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✔	
Creating or propagating computer viruses or other harmful files				✔	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✔	
On-line gaming (educational)	✔				
On-line gaming (non educational)		✔			
On-line gambling				✔	
On-line shopping / commerce		✔			
File sharing	✔				
Use of social media			✔		
Use of messaging apps			✔		
Use of video broadcasting eg Youtube	✔				

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour disciplinary procedures as follows:

ACTIONS AND SANCTIONS

Pupil Incidents	Refer to Class Teacher	Refer to E-Safety Co-ordinator	Refer to Executive Head or Head of School	Refer to Police	Refer to ICTDS for action re filtering/ security etc	Inform parents/ carers	Removal of network/ internet access rights	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✔	✔	✔		✔			✔
Unauthorised use of non-educational sites during lessons	✔	✔				✔	✔	✔	
Unauthorised use of mobile phone / digital camera / other mobile device		✔	✔			✔		✔	
Unauthorised use of social media / messaging apps / personal email		✔	✔		✔	✔	✔	✔	
Unauthorised downloading or uploading of files		✔	✔		✔	✔	✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔					✔	✔	
Attempting to access or accessing the school network, using another pupil's account		✔	✔			✔	✔	✔	
Attempting to access or accessing the school network, using the account of a member of staff		✔	✔		✔	✔	✔		✔
Corrupting or destroying the data of other users		✔	✔		✔	✔	✔		✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✔	✔			✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions		✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✔	✔			✔	✔		✔
Using proxy sites or other means to subvert the school's filtering system		✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident		✔	✔		✔	✔	✔		
Deliberately accessing or trying to access offensive or pornographic material		✔	✔	✔	✔	✔	✔		✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✔	✔	✔		✔	✔		

Staff Incidents	Refer to Executive Head or Head of School	Refer to Local Authority/ Governors/ HR	Refer to Police	Refer to ICTDS for action re filtering/ security etc	Warning	Possible Disciplinary Action	Possible suspension/ dismissal
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔			✔	✔
Inappropriate personal use of the internet / social media / personal email	✔			✔	✔	✔	
Unauthorised downloading or uploading of files	✔			✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔			✔	✔		
Careless use of personal data eg holding or transferring data in an insecure manner	✔				✔	✔	
Deliberate actions to breach data protection or network security rules	✔	✔		✔		✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔		✔	✔		✔	✔
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✔	✔		✔		✔	✔
Actions which could compromise the staff member's professional standing	✔	✔			✔	✔	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔			✔	✔	
Using proxy sites or other means to subvert the school's / academy's filtering system	✔	✔		✔		✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔	✔	✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔	✔		✔	✔
Breaching copyright or licensing regulations	✔				✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔				✔	

5. Security and Data Protection

The school and all staff members comply with the Data Protection Act (2018) and General Data Protection Regulation (GDPR) 2016. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for

staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.

6. E-Safety Complaints/Incidents

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Executive Headteacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated via the incident log form.

7. Review of Policy

This policy needs to be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated.