Date of approval: October 2018

Date of review: Autumn 2019

Signed:

Clenchwarton, Walpole Cross Keys & West Lynn Primary Schools Online Safety Policy October 2018

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- The school will identify a member of staff who has an overview of Online Safety, this would usually be the Designated Safeguarding Lead (DSL).
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually
- The Online Safety Policy was discussed by Staff on
- The Online Safety Policy was discussed by the School Council on:
- It was approved by the Governors on: _______________
- Date of next review:

Contents

Appendix 4 *- Parental/Carer Permission: Use of digital images – photography and video*

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Clenchwarton, Walpole Cross Keys and West Lynn Primary Schools, with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming *(sexual exploitation, radicalisation etc.)*
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours *(bullying)*
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being *(amount of time spent online, gambling, body image)*
- Sexting

- Copyright *(little care or consideration for intellectual property and ownership)*

Scope

This policy applies to all members of Clenchwarton, Walpole Cross Keys and West Lynn Primary Schools community *(including staff, students/pupils, volunteers, parents/carers, visitors, community users)* who have access to and are users of school technologies, both in and out of our schools

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and in the staffroom.
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate.
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource.
- Regular updates and training on online safety for all staff, including any revisions to the policy.
- ICT Code of Conduct *(previously referred to as an Acceptable Use Policy (AUP))* discussed with staff and pupils at the start of each year. ICT Code of Conduct/AUP to be issued to whole school community, on entry to the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not.
- Any concern about staff misuse is always referred directly to the Head Teacher, unless the concern is about the Head Teacher in which case the concern is referred to the Chair of Governors.

Review and Monitoring

The online safety policy is referenced within other school policies *(e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE policy).*

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

Our schools:

- have a clear, progressive online safety education programme *(SWGfL Digital Literacy Units)* as part of the digital literacy curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- will remind students about their responsibilities through the pupil ICT Code of Conduct
- ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, *e.g. use of passwords, logging-off, use of content, research skills, copyright*

Staff and governor training

Our schools:

- make regular up to date training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all staff information and guidance on the Online Safety Policy and the school's ICT Code of Conduct

Parent/Carer awareness and training

Our schools:

- provide information for parents/carers for online safety on the school website
- provide induction for parents which includes online safety
- runs a rolling programme of online safety advice, guidance and training for parents
- parents/carers are issued with up to date guidance on an annual basis

3. Incident management

In our schools:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed *(i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation)* in dealing with online safety issues

- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within our schools
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA and Trust
- for any breach of the acceptable use policy, the school will follow the agreed sanctions described in appendix 5 of this policy

4. Managing IT and Communication System

Internet access, security and filtering

In our schools:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision

E-mail

Our Schools:

- Provide staff with an email account for their professional use (nsix.org.uk) and makes clear personal email should be through a separate account
- We use anonymous e-mail addresses, for example head@, office@
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Pupils email:

- We use school provisioned pupil email accounts that can be audited
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School websites

- The schools web sites comply with statutory DfE requirements.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to ICT Code of Conduct

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our *[age appropriate]* pupil ICT Code of Conduct

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct and additional communications materials when required.

<u>5. Data Security</u>

Management Information System access and data transfer

- Teachers and office staff have access to the MIS (Pupil Asset).
- Data on this system must not be copied or shared with any other person and kept confidential.
- Staff must log out of the MIS when they are not near the computer.

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- Personal devices *(smartphones, laptops, personal tablets etc.)* should not be connected to the schools wifi.
- Pictures of children should not be taken on personal devices.
- Personal devices, other than smartphones, are discouraged from being brought into school.

Digital images and video

In our schools:

    - We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
    - We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs

- Staff sign the school's ICT Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment

Appendix 1a

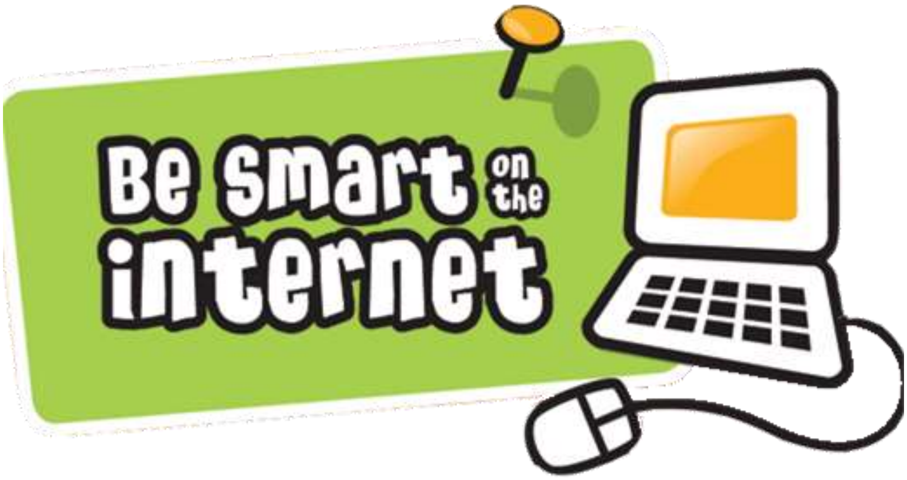
<u>Acceptable Use Agreement: EYFS & KS1 Pupils</u>

- I will ask a teacher or teaching assistant if I want to use the computers.
- I will only use activities that a teacher or teaching assistant has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or teaching assistant if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or teaching assistant if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I have read and understand these rules and agree to them.

Signed: …………………………………….. ***Date:…………………………………………..***

Name: ……………………………………… ***School: ………………………………………***



Appendix 1b

Acceptable Use Agreement: KS2 Pupils

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: ……………………………………   ***Date:…………………………………………..***

Name: ………………………………………   ***School: ………………………………………***

Appendix 2

ICT Code of Conduct Agreement (Staff/Governors/Visitors)

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by the West Norfolk Academy Trust. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with your line manager or DSL.

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, laptops and tablets

- All staff understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.

(Teaching Staff http://www.schoolspeoplenet.norfolk.gov.uk/Teaching-Staff/Working-in-a-Norfolk-School/Resolving-Issues/Disciplinary/index.htm
Support Staff http://www.schoolspeoplenet.norfolk.gov.uk/Support-Staff/Working-in-a-Norfolk-school/Resolving-Issues/Disciplinary/index.htm)

- All staff, Governors and visitors will not disclose any passwords provided to them by the school or other related authorities.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the permission of the Head Teacher.

- All staff, Governors and visitors understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Head teacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.

- All staff, Governors and visitors will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Body.

- All staff, Governors and visitors will ensure that all their school generated electronic communications are appropriate and compatible with their role.

- All staff, Governors and visitors will ensure that all data is kept secure and is used appropriately as authorized by the Head teacher or Governing Body. If in doubt they will seek clarification. This includes taking data off site.

- Personal devices must only be used in the context of school business with explicit permission of the Head Teacher.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system(s) for any school business

- Images will only be taken, stored and used for purposes in line with school policy. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head Teacher.

- All staff, Governors and visitors will comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Designated Safeguarding Lead (DSL) or Head Teacher in line with the school's Safeguarding Policy.

I acknowledge that I have received a copy, and agree to, the ICT Code of Conduct.

Full name:……………………………………………………………………..…

Job title:…………………………………………………………………………..…

Signature:…………………………………………………Date:……………………

Appendix 4

ICT Code of Conduct Agreement
(Parents/Carers)

Parent / carer name:………………………………………………

Pupil name: ……………………………………………………..

Pupil's class: ………………………………………

As the parent or carer of the above pupil(s), I grant permission for my child to have access to use the Internet, school email and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the ICT Code of Conduct/ Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy is available on the school website and that further advice about safe use of the Internet can be found via the school website.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, safe access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the websites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Carer signature:…………………………………………… Date:………………….

Use of digital images (photography & video)
Parent/Carers Agreement

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

- **If the pupil name is visible, we avoid using their photograph.**
- **If their photograph is used, we avoid using full names or identifying individual children.**
- **Where showcasing examples of pupils work we only use their first names, rather than their full names.**
- **We will only use pupil's first names in credits.**
- **Only images of pupils in suitable dress are used.**

Examples of how digital photography and video may be used include:

• Your child being photographed *(by the classroom teacher, teaching assistant or another child)* as part of a learning activity*; e.g. photographing children at work and then sharing the pictures through a projector/on screen in the classroom allowing the children to see their work and make improvements.*

• Your child's image for presentation purposes around the school; *e.g. in school wall displays and electronic presentations to capture images around the school or in the local area.*

• Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, *e.g. Our school website or the media.*

Use of digital images - photography and video:

I also agree to the school using photographs of my child or including them in video material. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent /Carer signature: ……………………………………………… Date: ………………..

Appendix 5

Sanctions for unacceptable use

- Parents will be informed immediately
- A temporary or permanent ban from Internet access
- A temporary or permanent ban from the use of school’s ICT facilities
- Access to the Internet may be withdrawn.
- A serious breach of the policy will result in further disciplinary action being taken, including suspension or expulsion.
- If it is suspected that a criminal offence has been committed the appropriate authorities will be informed
- Appropriate additional disciplinary action if the action breaks any other school rule or convention.
- This action will be defined in the Whole School Behaviour Policy and/or Anti-bullying Policy – Cyberbullying Policy
- Where applicable, referral to appropriate external agencies.

West Norfolk
Academies Trust