Carlton VC C of E Primary School

E Safety Policy

Approved by:	Mrs J Bevis and Governing Body	**Date:** 12/12/22	
Written by:	Mrs J Bevis	**Date :** 28/11/22	
Last reviewed on:			
Next review due by:	December 2024		

Carlton C of E Primary C of E Primary School
Policy for e-Safety

Introduction

The use of information and communication technology is an integral part of the national curriculum and is a key skill for everyday life. Computers, tablets, programmable robots, digital and video cameras are a few of the tools that can be used to acquire, organise, store, manipulate, interpret, communicate and present information. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Carlton C of E Primary School encourages use by pupils of the rich information and interactive resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. Access to on-line resources will enable pupils to explore thousands of libraries, databases and activities, and to exchange messages with people throughout the world.

Electronic information research skills are fundamental to the preparation of citizens and future employees. The school expects that staff will investigate possibilities and incorporate use of such information as appropriate within the curriculum; and that staff will provide guidance and instruction to pupils in the appropriate use of such resources. Staff will consult the ICT coordinator for advice on content, training and appropriate teaching levels consistent with the school's ICT programme of study.

We aim to remove any barriers, bias or discrimination that prevents individuals or groups from realising their potential and to provide equal opportunities and access to the curriculum for all children regardless of gender, age and cultural backgrounds, physical ability or special needs (See Equalities Scheme and Objectives).

At Carlton C of E Primary School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the 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.

This framework of e-safety and Acceptable Use Policy (AUP) is to promote safe and appropriate use. It should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

Given the array of new technologies now available to use for educational purposes and in everyday life, the intention of this policy is:

- To maximise e-Safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, iPads, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, iPads, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety Co-ordinator and Senior Information Risk Officer (SIRO) in our school is **Jo Bevis.** All members of the school community have been made aware of who holds these posts. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Staff and Governors are updated by the Head / e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

Information Classification

Restricted	**Protected**	**Public**
Personal information related to pupils or staff (contained in the Management Information System)	School routines, schedules and management information	Website and promotional materials. Display materials around school
Pupil reports	School Server – staff/admin	

e-Safeguarding Roles

SIRO (Senior Information Risk Owner)	**Mrs Jo Bevis**
IAO's (Information Asset Owner's)	**Mrs Lynne Pinfold** **Mrs Debra Barker**

Technician Responsibilities:
(Partnership Education)

Back-up server
Install new programs
Ensure Anti-Virus is up-to-date
Install updates
Keep servers and computers working correctly
Advise Headteacher of any issues/concerns

Access Controls

Restricted information:	**SIMS (Pupil and staff data)**	**Mrs Lynne Pinfold** **Mrs Debra Barker** **Mrs Jo Bevis**
	FMS(finance software)	**Mrs Lynne Pinfold** **Mrs Debra Barker** **Mrs Jo Bevis**

Protected information:	**School Server**	
	Staff areas	**Mrs Jo Bevis**
		Mrs Caroline Williams
		Mrs Aleshia Frost
		Mrs Ruth Fender
		Miss Jenny Rochford
		Miss Jasmine Notaro
		Ms Gingell
		Mrs Patricia Taylor
		Mrs Tricia Dickinson
		Mrs Lucy Worthington
		Ms Sarah Coxon
		Mrs Belinda Noah
		Mrs Naomi Muldowney
		Miss Rosie Ireland
		Mrs Nicola Collier
		Mrs Lynne Pinfold
		Mrs Debra Barker
	School Server	
	Admin areas	**Mrs Jo Bevis**
		Mrs Lynne Pinfold
		Mrs Debra Barker
	Governor Hub	**Mrs Jo Bevis**
		Mrs Hilary Tuohy
		Mrs Claire Bassett
		Mrs Emma Simpson
		Ms Katherine Wilkinson
		Mr John Kokot-Blamey
		Mrs Caroline Williams
		Rev'd Jacqueline Curtis
		Mrs Lynne Pinfold

E-Safety is a whole school issue; as such everyone within the school community has a responsibility to promote it including parents/carers supporting learning at home and ensuring all online work is supervised by a responsible adult.

This policy, supported by the school's acceptable use agreements for staff, governors, pupils and parents is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home–school agreements, behaviour and anti-bullying.

E-Safety skills development for staff

Staff receive regular information and training on e-Safety issues from the ICT / e-Safety coordinator.

New staff receive information on the school's acceptable use policy as part of their induction, then annually.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate e-Safety activities and awareness across the curriculum as appropriate.

E-Safety in the Curriculum

The school's internet access is controlled by filtering software chosen by the Local Authority, which should stop access to many inappropriate sites, although we recognise no system is totally secure.

Staff are aware that all inappropriate sites accidentally accessed in school should be reported to ICT Coordinator and then to the LA/E2Bn – incident to be logged.

Pupils will have supervised access to Internet resources (where reasonable).
Staff will preview any recommended sites before use.
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 this work. Parents will be advised to supervise any further research.

The school provides opportunities within a range of curriculum areas to teach about e-Safety. Pupils are aware of the impact of cyber bullying 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; i.e. parent/ carer, teacher/ trusted staff member.

The e-safety policy will be shared with the pupils at the start of each school year. Pupils and parents sign the AUP and internet permission slip.

The class teacher will provide appropriate guidance to pupils as they make use of the internet to enhance their learning.

Sanctions

Pupils deliberate violation of the AUP will result in a temporary or permanent ban on internet use. Additional action may be taken in line with the school's Behaviour Policy.

Password Security

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

Users are provided with an individual email and a Server log-in username.

Staff must :

- keep their password secure from pupils, family members and other staff and should choose alphanumeric passwords
- Use a different password for accessing school systems to that used for personal (non-school) purposes
- Change passwords regularly
- Log off or lock the computer using CTRL+ALT+DELETE when leaving unattended (The automatic log-off time for the school network is 10 mins.)

Starters and Leavers – The Headteacher / Office Staff will ensure that leavers' access is removed, or disabled, in a timely manner. Any school owned computer equipment (e.g. laptop) should be returned to the ICT Co-ordinator on staff exit. Starters will be given appropriate access to the school network on entry.

Anti-virus/anti-spam system

The school has an up to date anti-virus system which is installed when a device is delivered. This is automatically updated when a new release is available. Anti-spam is built in within the email platform and updates when a new release is available.

Where possible use of memory sticks and other mobile storage media should be restricted and scanned for viruses each time they are connected via a computer that is known to have the latest antivirus protection.

If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.

Data Security

The accessing of school data is something that the school takes very seriously. Access is via unique login and password and is restricted to necessary users.

Data accessed out of school (e.g. reports) is retrieved via password protected school email account / one drive.

Internet and Social Media

From the perspective of the School social media offers a new way to communicate key messages and engage with pupils, parents, governors and other stakeholders. It also offers the School opportunities for public consultation, a two way dialogue with pupils, staff, governors and parents for the purposes of influencing school policy and direction.

When using social media and internet sites the School will apply the same rules that would apply to the actions of employees in general as covered by the Safer Working Practices document and, therefore, draws no distinction between the conduct online and conduct offline. The School will take a view about staff actions in respect of social media and the internet either inside or outside of work that affect employee's work performance, the performance of others or the interests of the School.

Rights and Responsibilities

When using social networking sites and the internet staff should ensure that this does not damage the reputation of the School (or yourself) whether this is carried out during school time or privately. Staff are personally responsible for the content they publish on social media sites and the internet and must be mindful that this information will be in the public domain. Employees must have regard to the fact that they will be responsible for any commentary which is deemed to be a breach of copyright, defamatory, libellous or obscene.

Transparency

It is recognised that the line between professional and personal business can sometimes be blurred. It is important that individuals are thoughtful about the content and potential audiences for anything contributed to a social media site or the internet. It is vital that employees should be honest about their identity, and, where appropriate, be clear that any views shared are the employees as an individual and not necessarily the views of the School.

The use of social media on behalf of the School should only be used in a way that will add value to the School, and accordingly all employees have a duty to present accurate information and ensure that pupils, other staff, governors and parents are not misled.

Any member of staff contacted by the published media or radio or television about a post they have made on a social networking site should inform the Head teacher immediately.

Monitoring

While the School does not monitor employees through social networking sites or the internet if there were concerns with regard to the activities of a member of staff or an investigation was taking place then the School would consider accessing social media sites. This covers both private and professional use of social media.

Legal Issues

All employees of the School should take the following into consideration when using social media:-

- Be aware of the School policy and guidelines for using social media whether this is for personal use or as part of the working role.

- Be familiar with the legal areas outlined below before writing about colleagues or sharing information about the School.

- Ensure that posted material does not disclose privileged or confidential information.

- Remember that defamation is the act of making a statement about a person (or an institution) that is considered to harm their reputation. Where such a defamatory statement is written down (either in print or online) this is referred to as libel.

In drafting this policy the School recognises that it may be held responsible for something an employee has written or said if it is on behalf of the School or on a school sanctioned site. Action can also be taken against anyone repeating libellous information from another source so careful checks are needed before quoting statements from other social network sites or the internet.

Conclusion

The School respects the legal rights of employees with regard to the use of social networking and the internet. In general what an employee does in their own time is their affair and the School recognises that some staff may wish to publish private material on the internet including, but not limited to, social networking websites. Any activities, however, in or outside of work involving the internet are prohibited by this policy if they affect or could affect the School's reputation or service delivery interests, job performance (of the member of staff concerned or others) in a negative way in the reasonable opinion of the governors.

Employees may face disciplinary action if they harass, intimidate or demean other employees or stakeholders in the School on a social networking site. Employees must make every effort to ensure that any remarks on a social media website are credible and accurate with a disclaimer that the views are those of the member of staff and not of the employer. It is likely that to share confidential or private information about the School, its employees or governors on a social media site or the internet will result in a disciplinary investigation.

Email

Staff should use their individual school email address or the admin email address for school business
Under no circumstances should staff contact pupils or parents using personal email addresses.
Pupils in KS2 are introduced to email as part of the ICT Scheme of Work.
Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
Staff must inform the e-Safety co-ordinator if they receive an offensive e-mail.

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. The school **DOES NOT** allow a member of staff to contact a pupil or parent / carer using their personal device. Staff mobile devices must not be taken into the classrooms. Except for DDSL, when devices are needed to verify identity for CPOMS.

Pupils are not allowed to bring personal mobile devices/phones to school unless this is for educational purposes set by the teacher (even then, strict monitoring and controlled usage will only be permitted). Year 6 children may bring in a phone to left in the office during the day only if they are walking home by themselves and need it to contact a parent/carer.

The school is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any members of the school community is not allowed.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Safe Use of Images

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips. However with the express permission of the Headteacher, images can be taken provided they are transferred on return to school and solely, to the schools network and deleted from the staff device.

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the school office.

On a child's entry to the school, parents/carers will be asked to give permission to use their child's image. This consent form is considered valid for the entire period that the child attends this school. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Only the Web Administrators have authority to upload to the school website.
Images/ films of children are stored on the school's network.

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher. If used, material must be uploaded onto school system as soon as possible and deleted from mobile device.

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

ICT technician /coordinator have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Equal Opportunities - Pupils with additional needs

The class teacher and SEND coordinator will ensure that children with special educational needs will have additional support as required in order to develop their awareness and understanding of E-Safety and the AUP.

Parental Involvement

Parents/ carers and pupils are encouraged to contribute to adjustments or reviews of the school e-Safety policy.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school and then annually.

Parents/ carers are required to opt in whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

The school disseminates information to parents relating to e-Safety where appropriate through: Information evenings/ newsletters, school website.

Parents/carers supervise children during online learning.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Writing and Reviewing this Policy

Staff, pupils and governors have been involved in making/ reviewing the e-Safety policy through Staff Meetings, School Council and Governor meetings/liaison.

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Carlton C of E Primary School
Online/Internet Safety Rules
Pupil Acceptable Use Agreement

This applies to ALL online activity including any social media including or referring to school and school members.

- ✓ I will only use ICT in school for schoolwork and will only use sites my teacher has asked me to access.
- ✓ I will always ask the teacher before I use the Internet and will be sensible whenever I use it.
- ✓ I will only use my school email address when emailing and only email people my teacher has approved. The messages I send will be polite, sensible and responsible. .
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will not download programs or bring programs from home into school
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will **NEVER** give out my own details such as my name, phone number or home address on the Internet and I will tell the teacher if anyone asks me for my personal details.
- ✓ I will **NEVER** arrange to meet someone I have spoken to on the Internet
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I realise that if I don't use the Internet sensibly I will not be allowed to use it.

To: Carlton C of E Primary C of E Primary School

Acceptable Use Agreement and Parental Use of Photographs and Video

I / We have discussed the Pupil Acceptable Use Agreement and our

child ________________________________ (child's name) agrees to follow the Online/Internet

Safety Rules and to support the safe use of ICT at both School and at home.

Parent/Carer signature: ________________________Date:________.

Child's signature:_____________________Class :________________.

I have read, understood and will comply with the conditions of using photographs and video.

Parent/Carer signature: _________________________________

Print name_________________________________

Smile and Stay Safe Poster

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Carlton C of E Primary
Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

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 policy 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 policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Gail Highton, school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will take great care regarding social networks (e.g. Facebook) – Staff must not have any pupil (or former pupils) as 'on line' friends if they are of school age and any attempts by children to invite staff should be reported to School Safeguarding Officer. Staff / Governors must not make any mention of Carlton C of E Primary School on social media e.g. Facebook. Staff / Governors must ensure that any posts to social media are compatible with their professional role.
- I will not give out my own or colleagues personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email systems for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school when authorised by the Head or Governing Body.
- I will not install any hardware or software onto school PCs or laptops without permission of ICT coordinator
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent / carer, member of staff or Headteacher. All images should be uploaded to school server / printed and then deleted from device.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Staff laptops remain the property of the school, under no circumstances should pupils be given access to staff laptops for their learning

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature .... Date ....

Full Name ....(printed)

Job title . . . .

e-Safety Incident Log   Carlton C of E Primary C of E Primary School

Date/Time Location	Pupil/ Staff Name	Details of incident (incl. Evidence)	Immediate Action to minimise impact & reasons	Further Action (to prevent reoccurrence)	Any legal implications e.g. data protection act	Closed date

The Incident Log will be completed by the e-Safety Coordinator and monitored and reviewed termly and stored confidentially on the W drive (limited access by key staff only)

e-Safeguarding Risk Assessment Form –Carlton C of E Primary C of E Primary School

High Impact: Public exposure of restricted information leading to embarrassment, system downtime, or data corruption impacting learning & teaching.

Low Impact: Internal exposure **Medium Impact:** Exposure of protected information to a non-authorised third party, leading to outcomes listed above.

Information (restricted/ protected) taken out of school on laptop, email etc	Information accessed by external parties	2		Laptops taken out of school; Info sent via email	1		2	Use of secure email when appropriate / possible/password protect Use of school password protected, OneDrive – staff only
Use of mobile data storage e.g. memory sticks	Information accessed by external parties	2		Memory sticks taken out of school	1		2	USB sticks are **NOT** to be used for storing/transferring restricted/protected data – use of secure/password protected email or OneDrive
Use of Internet for data transfer and communication	Information accessed by external parties	2		n/a –use secure methods	1		2	Always use COLLECT, S2S, Anycomms – all secure
Pupil gaining access to restricted or protected information	Pupil gain access to teaching staff area	1		Staff leaves computer logged on and unlocked	2		2	Automatic locked screen after 10 minutes; staff advised to log off if leaving computer unattended
Remote access via school equipment or home computers	None to school server. Web based email accessed offsite via password by named staff	2		Web based email accessed offsite via password by named staff	1		2	Email only accessed via password offsite; secure emails require second password
Back up (storage)	Portable disc lost off site	2		Disc stored off site by named staff	1		2	Risk accepted; need back up offsite in case of critical incident
Password misuse or poorly managed	People access other users information	1		Use of computer in busy class – password may be seen	2		2	AUP in place; all pupils and staff reminded to never share passwords and to hide when

								entering
Viruses and malicious software installs	Disruption / unauthorised access to school data	2		Opening malicious emails; use of USBs (see above)	2		4	Anti virus and spam software updated automatically Ensure up to date with advice and guidance
Inadequate staff and pupil training in e-security and e-safety	Staff and pupils may not follow correct procedures	2		n/a	1		2	Staff and pupils regularly trained and constantly reminded of e-safety Begin each lesson with safety reminder
Remote online learning during self-isolation	Lack of parental supervision	2		Access to unsuitable material/sites	2		4	Provide information to parents in online safety, parental locks, up to date guidance

E-Safeguarding Action Plan Template – Carlton C of E Primary C of E Primary School

What will be done	*Resource Implications*	*Target Date(s)*	*Indicator of Success*	*Person Responsible*
Regular staff training	**time**	**ongoing**	**Staff confident in e-safety procedures Use of One Drive**	**Jo Bevis**
E-safety embedded throughout curriculum	**Time allocated in planning**	**ongoing**	**Pupils aware of how to stay e-safe and what to do if there is a problem**	**JB / class teachers**
Additional guidance for parental supervision	**Emails/Parentmail time**	**Regular reminders**	**Parents are aware of/confident in keeping children safe online**	**JB/admin**

E Safeguarding Procedures: Position at Autumn 2022

Procedure	In Place	Partially in place	Not in place	Don't know	Actions for consideration
Roles and Responsibilities: SIRO appointed, IAOs identified and listed, technician responsibilities specified	X				
1. Risk Assessment: Procedures established, assessments and remedial action plans documented	X				
2. Information Classification: Table created and system for classification labelling established	X				
3. Access Controls: *Systems access records* (who has access to what) and *Network security measures* established and implemented	X				
4. Use of ICT Systems: AUP 'owned' by everyone. On-going education & training programme for everyone	X				
5. Password Security: Minimum requirements in place	X				
6. Incident Reporting: Procedure in use and monitored with action taken as necessary	X				
7. Starters and Leavers: Procedures established and active for both staff and pupil records	X				
8. Remote Access: Minimum requirements in place	X				
9. Technical Security: Minimum requirements in place	X				