Carlton Primary School

Digital Literacy and Computing Policy

If you believe, you CAN achieve

1. Our Vision

At Carlton we see the use of technology as a key element of our curriculum. DLC skills are vital for our children as they continue their education and enter the working world.

We value the contribution that DLC can make for the benefit of all pupils, staff, parents and governors. We strive to provide safe DLC opportunities in all subjects to motivate and inspire pupils and raise standards across the curriculum. Everyone in our school community will become lifelong learners equipped to meet developing technology with confidence, enthusiasm and the skills that will prepare them for a future in an ever-changing world.

2. Overview

Teachers use the Interactive Whiteboards which are in every classroom to make their teaching visual, interactive and motivating. Pupils use our computer suite and our mobile laptop and iPad trolleys for many tasks within their learning. These range from research to art and publishing their work as well as computer programming. We make extensive use of digital photos and video for recording the children's learning and for publishing work.

3. Inclusion

- Pupils with special educational needs should be able to use the technology to encourage their independence and develop their interests and abilities.

- All pupils are to have access to the use of technology regardless of gender, race, cultural background or any physical or sensory disability. Pupils with learning difficulties can be given greater access to the whole curriculum through the use of technology.

- The youngest pupils in the Nursery and Reception classes begin to use and learn about DLC as soon as possible after entering school, so that they gain confidence in using computers as soon as possible.

4. Implementing the Policy

- The school uses the Switched On Computing scheme of work to support the planning and teaching of DLC

- Teachers ensure the teaching of DLC is evident within all areas of the curriculum following a topic based approach and creating cross curricular links.

- There are Interactive Whiteboards (IWBs) and Digital Visualisers in every classroom, used throughout the day for whole class teaching in all subjects. Whiteboards are also used in many group activities by teachers or TAs. Whiteboards are also regularly used by pupils themselves to participate in the class or group lesson, or demonstrate what they have learned or to display work they have done.

- The IWB is connected to a main classroom computer which is on the school network with its shared work area, and which also has access to the content and activities on the London Grid for Learning [LGfL] and Espresso Primary, and to the wider internet. Access to the internet is filtered by the Local Authority's service provider.

- There are 2 trolleys of 30 Chromebooks, which the children use for the majority of their DLC work.
- In addition, there are 2 laptop trolleys for use by pupils. Each trolley contains 15 laptops and there is one on each floor.
- There is a trolley of 16 iPads and two boxes of 10 iPads for use by all children across the school. In addition, Nursery and Reception have a set of 6 iPads.

- Teaching and support staff are confident selecting programs and make extensive use of resources for pupil to use from the school network, or online, particularly on Espresso Primary and the LGfL.

- The Leader of Learning for DLC regularly monitors teachers' planning for DLC, and observes the use of technology in lessons. These can be specific Computing lessons or from across the curriculum.

5. Developing and monitoring DLC

The Head teacher and Leader of Learning for DLC are responsible for ensuring there is a DLC policy and that it is implemented. The Leader of Learning for DLC is responsible for mapping the Scheme of Work and for liaising with other subject leaders to map the delivery of further DLC in learning and teaching across the curriculum.

Members of the SLT will monitor learning and teaching in DLC as they do for literacy and numeracy and other subjects.
The Leader of Learning for DLC will also be involved in monitoring class teachers' curriculum planning and teaching. An audit of staff skills will be carried out periodically by the Leader of Learning for DLC and support and training will be provided where necessary.

All staff will ensure that DLC is evident within classroom and curricular displays and in the class Floorbook.

The Leader of Learning will maintain an online portfolio showing progress across the school in key elements of the Computing National Curriculum.

6. Assessment

All teachers assess their pupils' attainment in DLC every term against the current level descriptors. This is then entered into the Primary Progress Toolkit as for other subjects.

7. Other relevant documents

- Appendix 1 : Online Safety Policy
- Appendix 2 : Acceptable Use Agreement for Staff
- Appendix 3 : Acceptable Use Agreement for Pupils

Appendix 1 Online Safety Policy

Contents

Key contacts

Carlton Primary School

Name of school/college:
Carlton Primary School

Headteacher/principal:
Name: Jacqueline Phelan
Contact details: head@carlton.camden.sch.uk

Online safety co-ordinator:
Name: Ted Glover
Contact details: ict@carlton.camden.sch.uk

Nominated LGfL contact:
Name:
Contact details:

IT systems/Data manager:
Name: Camden Schools IT Support Service
Contact details: educationit.support@camden.gov.uk

Designated safeguarding lead:
Name: Mandi Howells
Contact details: m.howells@carlton.camden.sch.uk

Nominated governor:
Name:
Contact details:

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO):
Name: Bodil Mlynarska
Contact details: 020 7974 6999

Child and Family Contact/MASH team:
Manager: Claire Mumby
Tel: 020 7974 1553/3317
Fax: 020 7974 3310

Camden online safety officer:
Name: Jenni Spencer
Tel: 020 7974 2866

London Grid for Learning resources available at:
https://www.lgfl.net/onlinonline safety/resource-centre?s=24

Rights Respecting School statement for policies

Carlton Primary School is beginning its journey as a Rights Respecting School, based upon the UNICEF Convention of the Rights of the Child. We believe that all children should grow up aware of these rights and respects these rights for themselves and for others. Being a Rights Respecting School will underpin policies throughout the school, and they will be reviewed and adapted throughout the 2017-18 academic year to demonstrate this.

1 Information on internet technology

1.1 Introduction

Carlton Primary School believes that the educational and social benefits for children in using the internet should be promoted, but that this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, we strive to teach children to keep themselves safe whilst online.
This document provides the Carlton Community with support for staff to recognise the risks and take action to help children use the internet safely and responsibly.

At Carlton, we ensure all our pupils, parents and staff are aware of our online safety policy through distribution to staff and regular online safety sessions for pupils. This document is also available on our school website: www.carlton.camden.sch.uk

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. The table shown at appendix 4 provides brief details of the various uses of the internet together with their benefits and risks.

As use of technology is now universal, it is imperative that children learn computing skills in order to prepare themselves for the working environment and that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as cyber bullying. More details on this can be found in section 4.5 of this policy.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- cyber bullying (see section 4.5 for further details)
- use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

2 School online safety strategies

2.1 Purpose and description

Computing is now a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of

Carlton's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

This policy ensures a safe e-learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

Through our robust practice, the use of the Switched On scheme for Computing and our PHSE lessons, Carlton will ensure the following is provided:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (for example the London Grid for Learning platform).

- A culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of on-line behaviour.

- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this is achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

2.2 Roles and responsibilities

2.2.1 Head teacher's role

Head teachers have ultimate responsibility for online safety issues within the school including:

- *the overall development and implementation of the school's online safety policy and ensuring the security and management of online data.*
- *ensuring that online safety issues are given a high profile within the school community*
- *linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy*
- *ensuring online safety is embedded in staff induction and training programmes*
- *ensuring online safety is embedded in the curriculum*
- *deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.*

2.2.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the head teacher in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

2.2.3 Online safety contact officer's role

Carlton's safeguarding contact officer is Mandi Howells. The Curriculum Leader for Digital Literacy and Computing is Ted Glover.

The safeguarding contact officer and DLC Leader have the authority, knowledge and experience to carry out the following:

- *develop, implement, monitor and review the school's online safety policy*
- *ensure that staff and pupils are aware that any online safety incident should be reported to them*
- *ensure that online safety is embedded in the curriculum*
- *provide the first point of contact and advice for school staff, governors, pupils and parents*
- *liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems*
- *liaise with the school's computing manager/co-ordinator to ensure they are kept up to date with online safety issues and to advise of any new trends, incidents and arising problems to the head teacher*
- *assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers*
- *raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature*
- *ensure that all staff and pupils have read and signed the acceptable use policy (AUP)*
- *report annually to the board of governors on the implementation of the school's online safety strategy*
- *maintain a log of internet related incidents and co-ordinate any investigation into breaches*
- *report all incidents and issues to Camden's online safety officer.*

2.2.4 Ted Glover, Curriculum Leader for DLC, will liaise with Camden Technicians to ensure the following takes place:

- *the maintenance and monitoring of the school internet system including anti-virus and filtering systems*
- *carrying out monitoring and audits of networks and reporting breaches to the online safety contact officer*
- *supporting any subsequent investigation into breaches and preserving any evidence.*

2.2.5 Role of school staff

All school staff at Carlton have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- *adhering to the school's online safety and acceptable use policy and procedures*
- *communicating the school's online safety and acceptable use policy to pupils*
- *keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet*
- *planning use of the internet for lessons and researching on-line materials and resources*
- *reporting breaches of internet use to the online safety contact officer*
- *recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety contact officer*
- *teaching the online safety and digital literacy elements of the new curriculum, primarily through the use of the Switched On Computing scheme.*

2.3 Pupils with special needs

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision.

SEND co-ordinators are responsible for providing extra support for these pupils and should:

- *link with the online safety contact officer to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with special needs*
- *where necessary, liaise with the online safety contact officer and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with special needs*
- *ensure that the school's online safety policy is adapted to suit the needs of pupils with special needs*
- *liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with special needs*
- *keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with special needs.*

2.4 Working with parents and carers

Carlton believes that parents and carers play a vital role in ensuring the safety of children using ICT and the internet.
Parents are aware of the curriculum through the school's website, where they also have access to the online safety policy. Parents are expected to sign an acceptable use agreement when their child starts at Carlton, and to support the school in upholding its points. In addition, parents are invited to attend coffee mornings to discuss online safety with representatives from the school and the local authority.
The CSCB online safety leaflet for parents is also available on the school website.

http://www.cscb-new.co.uk/downloads/esafety/E%20Safety%20-%20protecting%20your%20children%20on-line.pdf

3 Online safety policies

3.1 Accessing and monitoring the system

- *Access to the school internet system is via individual log-ins and passwords for staff and pupils wherever possible. Visitors should have permission from the head teacher or online safety contact officer to access the system and be given a separate visitors log-in.*

- *The school has access to a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.*

- *Network and technical staff responsible for monitoring systems are provided by Camden.*

- *Staff are required to regularly change their password.*

- *Internet-enabled devices are kept securely in trolleys and are only used with adult supervision.*

3.2 Confidentiality and data protection

- At Carlton, we will ensure that all data held on our IT systems is held in accordance with the principles of the Data Protection Act 1998. Data will be held securely and password protected with access given only to staff members on a “need to know” basis.

- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School. Any breaches of data security should be reported to the head teacher immediately.

- As the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.

3.3 Acceptable use policies

- *All internet users within the school are expected to sign an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.*

- *Staff are expected to sign an acceptable use policy on appointment [and annually after that] and this will be integrated into their general terms of employment.*

The online safety contact officer will keep a copy of all signed acceptable use agreements.

3.4 Teaching online safety

3.4.1 Responsibility

One of the key features of the school's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- *Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the online safety contact officer, but all staff play a role in delivering online safety messages.*

- *The online safety contact officer and DLC Leader are responsible for ensuring that all staff have the knowledge and resources to enable them to do so.*

- *Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.*

- *Rules regarding safe internet use are displayed in all classrooms and teaching areas where computers are used to deliver lessons.*

- *Teachers may also PSHE lessons as a forum for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line. Anti-bullying week is an example of when this may become a focus.*

3.4.2 Content

Pupils are taught all elements of online safety included in the computing curriculum so that they:

- *use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies*
- *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.*

3.4.3 Technology and sexual abuse and bullying behaviour

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. Schools need to be aware of the use of IT by older pupils for the

purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this.

For example, sexting involves the sending of intimate photographic images of an individual to others electronically via the internet. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

On-line behaviour that involves sexual abuse and bullying is a criminal offence, although it is unlikely that the perpetrator will be prosecuted where it is a peer of the victim.

Carlton will make a referral to Family Services and Social Work for any pupil who displays sexually abusive behaviour towards other pupils.

3.5 Staff training and conduct

3.5.1 Training

- All school staff and governors receive training with regard to IT systems and online safety as part of their induction.
- Staff also attend specific and regular training on online safety from accredited trainers, in partnership with the CLC.

3.5.2 IT and safe teaching practice

Staff at Carlton are aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.
The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- *Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.*

- *Staff should always use school equipment and only store images on the school computer system, with all other copies of the images on personal mobile devices erased.*

- *Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.*

- *Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.*

- *Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.*

- *Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.*

- *Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.*

- *When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.*

- *When making contact with parents by email, staff should always use their school email address or account. Personal email addresses and accounts and social networking sites should never be used.*

- *Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.*

- *Where staff are using mobile equipment such as laptops or i-pads provided by the school, they should ensure that the equipment is kept safe and secure at all times. Staff who have a personal i-pad for school use sign a separate agreement.*

3.5.3 Exit strategy

When staff leave, the school will ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

3.6 Safe use of technology

3.6.1 Internet and search engines

- *Carlton believes that children should be supervised at all times when using the internet.*

- *Pupils are not allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.*

- *Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers plan use of internet resources ahead of lessons by checking sites and using education-specific resources, such as those provided by LGFL.*

- *Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety contact officer, who will liaise with the IT service provider for temporary access. Teachers should notify the online safety contact officer once access is no longer needed to ensure the site is blocked.*

3.6.2 Evaluating and using internet content

Teachers at Carlton teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

***The School email system** is hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally. At present, pupils do not have email addresses.*

***Social networking sites** such as Facebook, MySpace and Twitter are blocked in school, but we are aware that many pupils have access to these at home so they are included in our online safety learning.*

***Newsgroups, chat rooms and forums** are mostly blocked by the LGFL policy.*

***Gaming-based sites** allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites are not accessible via school internet system.*

***YouTube** is a video hosting site that Carlton feels has many educational uses. Teachers are required to log in with their LGFL USO in order to access it, and will watch videos before using them in lessons in order to ensure they are appropriate.*

Safety rules

- *Pupils are taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.*

- *Pupils are warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.*

- *Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.*

- *In order to help pupils to stay safe online outside of school, they are taught:*

    - *not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended*
    - *to only use moderated chat rooms that require registration and are specifically for their age group;*

- *not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them*
- *how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them [dependent on age]*
- *to behave responsibly whilst on-line and keep communications polite*
- *not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.*
- *not to give out personal details to anyone on-line that may help to identify or locate them or anyone else*
- *not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room*
- *to behave responsibly whilst on-line and keep communications polite*
- *not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.*

3.6.4 Video conferencing (where appropriate)

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- *Teachers should try to use a safe video conferencing platform, ie: London Grid for Learning and need to be aware of the risks associated with live video feeds.*

- *Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call.*

3.6.5 School website

- *Content is not uploaded onto the school website unless it has been authorised by the online safety contact officer and the head teacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.*

- *Carlton has designated members of admin staff who have responsibility for uploading materials onto the website.*

- *To ensure the privacy and security of staff and pupils, the contact details on the website are the school address, email and telephone number. No contact details for staff or pupils are contained on the website.*

- *Children's full names are never be published on the website.*

- *Links to any external websites will be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.*

3.6.6 Photographic and video images

- *Where the school uses photographs and videos of pupils for publicity purposes, group photographs are mainly used.*

- *Where photographs or videos of children are used, written permission is obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.*

- *Children's names are never published where their photograph or video is being used.*

- *Images should be securely stored only on the school's computer system and all other copies deleted.*

- *Staff should not use personal devices to take photographs of pupils.*

- *Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.*

3.6.7 Pupils' own mobile devices

Mobile devices are not allowed in classrooms and any pupils bringing them into school, e.g. those in Year 6 who walk home on their own, must hand them in to the school office for secure storage until the end of the day.

4 Responding to incidents

4.1 Policy statement

- *All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety contact officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety contact officer on the online safety incident report form (appendix 3).*

- *A copy of the incident record should be emailed to Camden's designated online safety officer at jenni.spencer@camden.gov.uk.*

- *Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action and consideration given to contacting the LADO where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors.*

- *The school's online safety contact officer should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.*

- *Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher, who will make a decision as to whether or not to refer the matter to the police and/or Family Services and Social Work in conjunction with the head teacher.*

Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- *If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.*

- *Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.*

- *The incident should be reported to the online safety contact officer and details of the website address and URL provided.*

- *The online safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.*

4.3 Intentional access of inappropriate websites by a pupil

- *If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).*

- *The incident should be reported to the online safety contact officer and details of the website address and URL recorded.*

- *The online safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.*

- *The pupil's parents should be notified of the incident and what action will be taken.*

4.4 Inappropriate use of IT by staff

- *If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the online safety contact officer immediately. If the misconduct involves the head teacher or governor, the matter should be reported to the chair of the board of governors.*

- *The online safety contact officer or DLC Leader will notify the network manager so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.*

- *The online safety contact officer or DLC Leader will arrange with Camden IT to carry out an audit of use to establish which user is responsible and the details of materials accessed.*

- *Once the facts are established, the head teacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.*

- *If the materials viewed are illegal in nature the head teacher or governor should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.*

4.5 Cyberbullying

4.5.1 Definition and description

Cyberbullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, sexting/"happy slapping").

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- *School anti-bullying and behaviour policies and acceptable use policies cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.*

- *Any incidents of cyber bullying should be reported to the online safety contact officer who will record the incident on the incident report form and ensure that the*

incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.

- *Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.*

- *As part of online safety awareness and education, pupils will be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.*

- *Pupils should be taught:*

    - *to only give out mobile phone numbers and email addresses to people they trust and with parent or carer's permission*
    - *to only allow close friends whom they trust to have access to their social networking page*
    - *not to send or post inappropriate images of themselves*
    - *not to respond to offensive messages*
    - *to report the matter to their parents and teacher immediately.*

- *Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.*

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- *Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The pupil should also consider changing their phone number.*

- *Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The pupil should also consider changing email address.*

- *Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.*

- *Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.*

- *Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.*

4.5.4 Cyberbullying of teachers

- *Head teachers should be aware that teachers may become victims of cyberbullying by pupils and/or their parents. Because of the duty of care owed to staff, head teachers should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents.*

- *The issue of cyberbullying of teachers should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.*

- *Incidents of cyber bullying involving teachers should be recorded and monitored by the online safety contact officer in the same manner as incidents involving pupils.*

- *Staff should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.*

- *Personal contact details for teachers should not be posted on the school website or in any other school publication.*

- *Staff should follow the advice above on cyberbullying of pupils and not reply to messages but report the incident to the head teacher immediately.*

- *Where the bullying is being carried out by parents the head teacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.*

4.6 Sexting and sexual abuse and harassment by peers

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying.

“Sexting” or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Schools need to be aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this.

On-line behaviour that involves sexual abuse and bullying is a criminal offence, although it is unlikely that the perpetrator will be prosecuted where it is a peer of the victim.

However, schools need to include responses to sexual bullying in their behaviour policy and make a referral to Children's Safeguarding and Social Work for any pupil who displays sexually abusive behaviour towards other pupils. Staff should refer to Camden's "Children who harm other children" guidance for further details on this. http://www.cscb-new.co.uk/downloads/policies_guidance/local/Children%20who%20harm%20other%20children%20protocol.pdf

Schools should also be aware of when any of these behaviours may be linked to the sexual exploitation of a pupil or is being carried out as a gang-related activity. Staff should refer to the CSCB child sexual exploitation guidance for further details. http://www.cscb-new.co.uk/wp content/uploads/2015/09/Multi_Agency_Guidance_On_Child_Sexual_Exploit tion_2015.pdf

4.6 Risk from inappropriate contacts with adults

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of pupils being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records. The perpetrators may be adults but may also be peers.

- *All concerns around inappropriate contacts should be reported to the online safety contact/child protection officer [Mandi Howells].*

- *The designated child protection officer should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Family Services and Social Work and/or the police.*

- *The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.*

- *The designated child protection teacher can seek advice on possible courses of action from Camden's online safety officer in Family Services and Social Work.*

- *Teachers will advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.*

- *The designated child protection teacher and the online safety contact officer should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.*

- *Where inappropriate contacts have taken place using school IT equipment or networks, the online safety contact officer should make a note of all actions taken and contact Camden IT to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.*

4.8 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result.

All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- *Through training, staff will be made aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.*

- *The school will ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.*

- *All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.*

- *The online safety co-ordinator and the designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.*

- *Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer the young person to the Channel Co-ordinator for support.*

4.8 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- *Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor*

- *Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.*

5 Sanctions for misuse of school IT

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- *use of non-educational sites during lessons*
- *unauthorised use of email or mobile phones*
- *unauthorised use of prohibited sites for instant messaging or social networking.*

At Carlton the class teacher should be notified immediately. The child should be informed that the safety officer will be informed who will wish to discuss the incident with them. The sanction may result in red letter and parents notified. The online safety officer will complete an incident form based on the class teacher's incident form.

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- *continued use of non-educational or prohibited sites during lessons*
- *continued unauthorised use of email, mobile phones or social networking sites during lessons*
- *use of file sharing software*
- *accidentally corrupting or destroying other people's data without notifying staff*
- *accidentally accessing offensive material without notifying staff.*

At Carlton the class teacher should be notified immediately. The child should be informed that the safety

officer will be informed and will need to discuss the incident with them. The sanction may result in red letter and parents notified. The online safety officer will complete an incident form with the child and parent where possible. Child to receive no ICT free time during sessions for the term.

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- *deliberately bypassing security or access*
- *deliberately corrupting or destroying other people's data or violating other's privacy*
- *cyber bullying*
- *deliberately accessing, sending or distributing offensive or pornographic material*
- *purchasing or ordering items over the internet*
- *transmission of commercial or advertising material.*

At Carlton the head teacher/online safety officer should be notified immediately. The sanction may result in an internal exclusion or fixed term exclusion. Parents contacted to attend school immediately. The head teacher/online safety officer will complete an incident form with the child and parent where possible and send it to Camden Online safety Officer within 24hrs. Child to receive fixed period ban from access to Internet and school ICT equipment.

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- *persistent and/or extreme cyber bullying*
- *deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent*
- *receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act*
- *bringing the school name into disrepute.*

At Carlton the head teacher/online safety officer should be notified immediately. The sanction will result in fixed term exclusion. Parents contacted to attend school immediately. The head teacher/online safety officer will complete an incident form with the child and parent where possible and send it to Camden Online safety Officer within 24hrs. Child to receive fixed period ban from access to Internet and school ICT equipment.
Referral to police and Camden's online safety officer for family support and possible individual pupil support from services. Depending on outcome, potential permanent exclusion from school.

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by

staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher.

- *excessive use of internet for personal activities not connected to professional development*
- *use of personal data storage media (eg: removable memory sticks) without carrying out virus checks*
- *any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites*
- *sharing or disclosing passwords to others or using other user's passwords*
- *breaching copyright or licence by installing unlicensed software.*

Sanctions include referral to the head teacher who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO.

- *serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications*
- *any deliberate attempt to breach data protection or computer security rules, for example hacking*
- *deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent*
- *receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act*
- *bringing the school name into disrepute.*

Sanctions include:

- referral to the head teacher
- removal of equipment
- referral to Camden's online safety officer
- referral to SSC or police
- suspension pending investigation
- disciplinary action in line with school policies

Head teacher informs Chair of Resources Committee of investigation. Following outcome discusses consequences with Chair and disciplinary actions taken. Chair of Governors will not be involved at this stage to remain independent for appeals purposes.

Appendix 2

Carlton Primary School

Acceptable Use of Technology Policy for Staff 2016-17

1. I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or Camden LEA) into disrepute.

2. I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group. 4. I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

5. Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.

6. I will not trespass into other users' files or folders.

7. I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.

8. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Ted Glover/Camden Schools IT Support .

9. I will ensure that I log off after my network session has finished.

10. If I find an unattended machine logged on under other users username I will not continuing using the machine – I will log it off immediately.

11. I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.

12. I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.

13. I will not use the network in any way that would disrupt use of the network by others.

14. I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to Ted Glover/Mandi Howells.

15. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

16. I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.

17. I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.

18. I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.

19. I will support and promote the school's online safety and safeguarding policies and help students be safe and responsible in their use of the Internet and related technologies.

20. I will ensure that portable ICT equipment such as laptops, iPads, digital still and video cameras are securely locked away when they are not being used.

_____

I have read the above policy and agree to abide by its terms.

Name: _____

Signed: _____ Date: September 2016

Appendix 3

Carlton Primary School

Acceptable Use of Technology Policy for Pupils 2016-17

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep any passwords I have a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend or without my parents/carers' permission
- talk to my teacher before using anything on the internet that I'm unsure about
- not tell people about myself online (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Wasting time or resources on school computers.

I have read these rules, I understand them and I will follow them.

Signed: _____ Class:_____