Frank Barnes School for Deaf Children

Online Safety and Social Media Policy

Frank Barnes
School for Deaf Children

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO):

Name: Sophie Kershaw

Contact details: 020 7974 4556

Child and Family Contact/MASH team:

Manager: Jade Green

Tel: 020 7974 1553/3317

Fax: 020 7974 3310

Camden online safety officer:

Name: Jenni Spencer

Tel: 020 7974 2866

Prevent Education Officer

Name: Jane Murphy

Tel: 020 7974 1008

Contents Page

1. INFORMATION AND INTERNET TECHNOLOGY

1.1 Introduction

It is commonly acknowledged 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, schools need to be able to teach children to keep themselves safe whilst on-line.

This document provides schools with guidance on developing an effective online safety strategy to enable these aims to be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

At Frank Barnes School, we provide the following guidance to achieve this by helping our school community to recognise the risks and take action to help our children use the internet safely and responsibly.

We ensure that we communicate the online safety policy to staff, pupils and parents and this document is posted on the school's website.

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 5 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.

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 as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school'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.

Schools should consider the following in order to ensure a holistic approach to online safety:

- Staff should be aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and should be aware of the use of technology in peer on peer abuse.

- When developing new policies, schools should ensure online safety and the impact of technology is considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.

- Schools should ensure that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff should receive suitable training around online safety and similar messages should be taught to pupils.

- Staff should be aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with pupils, and schools must ensure there are clear policies available to staff on expectations for online behaviour.

- There should be a clear link between the online safety policy and the behaviour policy that sets out expected standards for pupil's online behaviour and expected sanctions for breaches.

- School's online safety policies should be reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

Schools should refer to:

DfE non-statutory guidance on teaching online safety:

https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE:

https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

2.2 Purpose and description

Schools should have an online safety strategy in place based on a framework of policy, practice, education and technological support that 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.

In particular, schools must ensure the following:

- 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 should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

The school has an online safety team compromising of Katherine O'Grady and Dani Sive. It is the responsibility of the team to ensure the implementation of the policy and online safety incidents. The online safety coordinator is Katherine O'Grady.

2.3 Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole school community, including teaching assistants, supervisory assistants, governors and others, and forge links with parents and carers. The strategy must have the backing of school governors, should be overseen by the head teacher and be fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Headteacher'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 online safety is embedded in the curriculum
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

2.3.2 Governor's 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.

2.3.3 Online safety co-ordinator's role

The designated online safety officer is Katherine O'Grady, she is responsible for coordinating online safety policies on behalf of the school. Ideally, the contact officer should be a senior member of the management team. Given the issues associated with online safety, it is appropriate for the designated child protection teacher to be the school's online safety contact officer.

The online safety contact officer should 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 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.

In addition, it is an Ofsted recommendation that the online safety contact officer receives recognised training CEOP or E-PICT in order to carry out their role more effectively. In Camden, this is available from the CLC.

2.3.4 Network manager's role

Where schools have one, their role is:

- 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.

Where schools do not have an IT manager, support and advice can be provided and the head teacher or a delegated staff member needs to take responsibility for organising this.

2.3.5 Role of school staff

All school staff 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 as part of the new Computing curriculum

2.3.6 Designated Safeguarding/Leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection teacher for the school who will decide whether or not a referral should be made to Family Services and Social Work or the Police. In some schools, the designated child protection teacher will be the online safety contact officer.

2.4 Pupils with special educational needs and disabilities (SEND)

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. Schools should have a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

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 need
- 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

It is essential that schools involve parents and carers in the development and implementation of online safety strategies and policies; most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The school should consider offering online safety training opportunities to parents in order to provide them with information to help them keep their child safe online. The Camden Safeguarding Children Partnership (CSCP) online safety leaflet for parents should also be available on the CSCP website: https://cscp.org.uk/parents-and-carers/online-safety/

The headteacher, board of governors and the online safety contact officer should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Parents should be provided with information on computing and the school's online safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Parents should also be informed that they can contact the school's online safety co-ordinator if they have any concerns about their child's use of technology.

3. ONLINE SAFETY POLICIES

3.1 Accessing and monitoring the system

- Access to the school internet system should be 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 online safety contact officer should keep a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.
- Staff should be required to change their password every 6 months.
- Network and technical staff responsible for monitoring systems should be supervised by a senior member of their management team.
- The online safety contact officer and teaching staff should carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

3.2 Confidentiality and data protection

- The school will ensure that all data held on its 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.
- Where 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 will be 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.
- For primary school pupils, acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet in school (see appendix 1).
- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 3).

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

3.4 Teaching online safety

When developing the teaching of online safety, schools should have regard to the Department of Education guidance Teaching online safety in schools available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

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 should play a role in delivering online safety messages.
- The online safety contact officer is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.
- The online safety co-ordinator should ensure that any external resources used for teaching online safety have been thoroughly reviewed in advance.
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Teachers may wish to use PSHE lessons and during statutory relationships and sex education 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.
- Schools should teach online safety in a safe environment that allows pupils to discuss issues in an open, honest and non-judgemental way and it is recommended that the designated safeguarding lead is involved in the development of any lessons teaching online safety.

- As these discussions may lead to pupils recognising that they have been harmed online, teachers should be aware that following discussions, pupils may wish to make a disclosure.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.

3.4.2 Content

The teaching of online safety should focus on:

- how to critically evaluate and make judgements on online content
- how to recognise techniques used to persuade or manipulate, for example extremist views, grooming and targeted marketing
- what is and is not acceptable online behaviour
- identifying online risks
- how to get help and support.

Pupils should be 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.

Teaching online safety should enable pupils to:

- understand the specific harms and risks inherent in using the internet, for example how people can behave differently on the internet and how the internet can be used to magnify and distort information and provide a platform for "fake news" and extremist views;
- how to stay safe online, how to identify online harm and abuse and what actions to take report this.

3.5 Staff training and conduct

3.5.1 Training

- All school staff and governors should receive training with regard to IT systems and online safety as part of their induction and this should include a meeting with the online safety co-ordinator and the network manager.
- Staff should also attend specific training on online safety available from the CSCB (https://cscp.org.uk/training/) so that they are aware of the risks and actions

to take to keep pupils safe online. School management should ensure that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

Camden City Learning Centre offers whole school training including updates as well as training for governors and parents.

3.5.2 IT and safe teaching practice

School staff need to be 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. Staff should refer to the model social media policy for school staff for further guidance.

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 must always use school equipment and only store images on the school computer system. No photos allowed on personal mobile devices.
- 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.
- Where staff need to communicate with pupils regarding school work, this should be via the school lgfl (London Grid for Learning) email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.
- 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 or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts such as SN (Social Networking) 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.

3.5.3 Exit strategy

When staff leave, their line manager should liaise with the network manager to 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

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.
- Primary school children should be supervised at all times when using the internet. Although supervision of secondary school pupils will be more flexible, teachers should remain vigilant at all times during lessons.
- Pupils should not be 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, staff should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- 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 should 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

School email systems should be 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.

Social networking sites such as Facebook, MySpace and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

Chat rooms are internet sites where users can join in "conversations" on-line;

Instant messaging allows instant communications between two people on-line. In most cases, pupils will use these at home although school internet systems do host these applications.

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 should not be accessible via school internet systems

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is

forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- If schools identify a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.
- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher e.g. year 6 pupils to learn the use of emailing system as part of the computing curriculum.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety contact officer who will liaise with the learning platform provider.
- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Pupils should be 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.
- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.
- Pupils should be 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 teach pupils to stay safe online outside of school, they should be advised:

    - 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
    - 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

Video calling or live streaming enables users to communicate face-to-face via the internet using web cameras.

Schools should have a remote learning policy and should refer to the DfE and London Grid for Learning guidance for advice on what to include. The following shou;d be taken into account:

https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- *only using school registered accounts rather than personal accounts*
- *recording remote learning for safeguarding purposes*
- *the security of the video link*
- *checking settings regularly to ensure teachers have full control of the meeting ie; who can start, join or chat in the stream*
- *paying attention to background settings to prevent breach of privacy*
- *training for teachers to use the new technology*
- *a system for teachers to log any remote learning contacts and issues.*

Further guidance on remote learning can be found on the London Grid For Learning website: https://www.lgfl.net/online-safety/

3.6.5 School website

- Content should not be 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.
- Schools should designate a named person or persons to have responsibility for uploading materials onto the website. This is particularly important where a school allows a number of staff members to upload information onto the website.
- To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website.
- Children's full names should never be published on the website.

3.6.6 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.
- Where photographs or videos of children are used, written permission must be 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 should never be published where their photograph or video is being used.
- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.
- Images should be securely stored only on the school's computer system and all other copies deleted.
- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

- 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

The majority of pupils are likely to have mobile phones or other devices that allows them to access internet services, and these can pose a major problem for schools in that their use may distract pupils during lessons and may be used for online bullying.

However, many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. Generally, use of personal mobile phones or other devices should be forbidden in classrooms.

Schools need to be aware that it is considerably more difficult to monitor wireless devices and this should be considered when deciding on the school policy around pupils bringing in and using their own devices. This will also apply to handheld devices such as i-pads that are given to pupils by schools for education purposes.

If schools will allow pupils to access the school internet system via their own devices, it must be made clear to pupils that the same acceptable use agreements apply and that sanctions may be applied where there is a breach of school policy.

Schools should also consider what policy to apply to staff use of their own devices whilst at school.

Where a pupil's device is used for bullying or sexual harassment, schools should have a policy in place allowing the device to be confiscated so that evidence can be gathered. Schools should refer to the government guidance available at:

https://www.gov.uk/government/publications/searching-screening-and-confiscation

Individual schools should record their policy here:

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 4).

- 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 under staff conduct policies for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff 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 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 will arrange with the network manager or learning platform provider 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 Online bullying

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. All incidents should be dealt with under the schools' behaviour policies and the peer on peer abuse guidance. https://cscp.org.uk/professionals/schools-and-nurseries-safeguarding-policies/

- School anti-bullying and behaviour policies and acceptable use policies should 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 notify 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 should 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

    - 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.

Any action taken on cyber bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions. This may be facilitated by the School Council or a specialist resource such as Cybermentors.

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 Online Bullying of school staff

- 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.
- Teachers 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 Harmful sexual behaviour online

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.

Schools should be aware of online behaviours of a sexual nature that could constitute harmful behaviour:

- sharing explicit and unwanted content and images
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats.

Schools also need to be aware of the issue of "upskirting" where pictures are taken of under a person's clothing without them knowing in order to view their genitalia or buttocks with a view to sharing the images in order to distress or humiliate the victim. This is now a criminal offence.

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.

Schools should be aware of the duty under statutory guidance *Keeping children safe in education* and *Sexual violence and sexual harassment between children in schools and colleges* which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCP *Sexually harmful behaviour protocol* for further details. https://cscp.org.uk/resources/sexual-harmful-behaviours/

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 CSCP child sexual exploitation guidance for further details. https://cscp.org.uk/resources/child-sexual-exploitation-resources/

4.7 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 officer and the designated child protection teacher.
- The designated child protection teacher 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 the network manager or learning platform provider 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.

4.7 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.

- Staff need to be 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 should 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 contact officer and the designated child protection teacher 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.
- If there is evidence that the pupil is becoming deeply enmeshed in the extremist narrative, schools should seek advice from Camden's Integrated Youth Support Services on accessing programmes that prevent radicalisation. Where there is evidence that their parents are involved in advocating extremist violence, referral should be made to LADO.

4.8 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of developing grievance, promoting extremist thought and division. They can use this to justifying verbal or physical violence against another group. Terrorist groups may also use the internet and social media to provide information on preparing explosives or carrying out terrorist acts. Some young people may be particularly vulnerable, lack resilience and so be more susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

The Prevent Duty requires all schools to prevent young people from being radicalised and drawn into terrorism. Schools need to consider how their leadership and management, school ethos and curriculum including online safety supports with building children's resilience to any radicalising influences. All Local Authorities are required to have a Channel Panel which offers a voluntary support package to individuals who have been referred due to a particular vulnerability. This is a multi-agency panel with a variety of interventions on offer to the to encourage critical thinking, stop the radicalisation process and divert them from extremism.

- *All school staff who use the internet as part of their lessons need to be aware of their responsibilities to promote good conduct, support young people to be aware of the dangers of contact and how to put security in place and how to recognise and report inappropriate content. This is part of building young people resilience which is one of the 6 strands of the Prevent Duty*

- *Staff need to be 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 know of the risks of becoming involved in groups with extremist ideologies and the tactics they may to groom and exploit. Staff and young people should also be made aware that accessing and sharing certain content is against school policies and certain contact with certain groups is illegal.*

- *The school should ensure that adequate electronic filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism. Schools also need to ensure that other filtering methods are in place eg. Consideration of how the internet is accessed in school and which staff are available to support. Also children should be able to support one another to filter content and report concerns they have for each other.*

- *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 to MASH. If there is imminent danger dial 999. In all other circumstances follow the schools safeguarding procedures by speaking to the DSL. If next steps are not clear speak to the Prevent Education Manager or refer directly to MASHadmin@camden.gov.uk*

Schools may contact the Prevent Education Manager for advice on any of the above.

Further information is available in the CSCP guidance "Safeguarding children and young people from radicalisation and extremism" available at: https://cscp.org.uk/resources/radicalisation-and-extremism-resources/

4.9 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.

- The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.

- 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

Individual schools are responsible for deciding what sanctions will be applied for breach of acceptable use policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors. The following is a framework recommended by LGfL that schools may want to adopt: For each point, schools may record their own detailed list of breaches and corresponding sanctions.

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.

Sanctions could include referral to the class teacher or tutor as well as a referral to the online safety contact officer.

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.

Sanctions could include:

- referral to class teacher or tutor

- referral to online safety contact officer
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

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.*

Sanctions could include:

- *referral to class teacher or tutor*
- *referral to online safety contact officer*
- *referral to head teacher*
- *loss of access to the internet for a period of time*
- *contact with parents*
- *any sanctions agreed under other school policies.*

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.

Sanctions could include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's online safety officer.

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. *Sanctions will be linked to the staff behaviour policy or code of conduct.*

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 *as a low level incident in line with the school's staff conduct policy.*

.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (e.g. 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.

Possible 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 *under the CSCP guidance on dealing with allegations against staff and volunteers.*

https://cscp.org.uk/professionals/managing-allegations-against-staff-and-volunteers-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.

Possible sanctions include:

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

6. SOCIAL MEDIA

Social media refers to web based social networks, internet forums and blogs, such as Facebook, Instagram, Pinterest, and Vine. Given the rapid expansion of social media, it is impossible to list all possible types of media as they are constantly evolving and multiplying.

School staff should assume that all online activity is covered by this policy and should follow these guidelines in relation to any social media that they use, both at work and to an extent in their personal situation.

While acknowledging the benefits of social media and the internet it is also important to recognise that the risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal; and Frank Barnes has this policy in place to deal with any misuse of social media.

6.1 Objectives

This policy takes account of all the appropriate legislation and sets out to:

- Assist those who work with pupils to work safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils.
- Offer guidance on utilising social media for educational, personal and recreational use.
- Advise that, in the event of unsafe and/or unacceptable behaviour arising from the inappropriate use of social media, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practices and minimise the risk of malicious allegations against staff colleagues and others who have contact with pupils at the School.

6.2. The Use of Social Media within the School

School staff are not permitted to access social media websites from the School's computers or other school devices at any time, unless authorised to do so by a member of the School leadership team.

However, staff may use their own devices to access social media websites while they are in the school, outside of teaching or PPA time. Excessive use of social media, which could be considered to interfere with school's productivity and providing an education service, and could therefore be considered as a misconduct matter, and subject to the school's disciplinary policy and procedure.

Staff should assume that any content they write (regardless of their privacy settings) could become public. Therefore, they should ensure that any content they produce is professional, maintaining a clear distinction between their personal and professional school lives.

Any use of social media made in a professional capacity must not:

- bring the school into disrepute;
- breach confidentiality;

- breach copyrights of any kind;
- bully, harass or be discriminatory in any way;
- be defamatory or derogatory.

6.3. Use of Social Media Outside of School

The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their user profile as being associated with the School, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, they should avoid mentioning the school by name, or any member of staff by name or position or any details relating to a pupil of the school. Opinions offered should not bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

6.4 General Considerations

When using social media whether at work or outside of work staff and others within the school should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses or other personal data to pupils or parents or any other party.
- not have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites
- Not to have any online friendships with any young people under the age of 18, unless they are family members or close family friends.
- Not to have online friendships with parents or carers of pupils, or members of the governing body/trustees.
- Take personal responsibility for what they communicate in social media and bear in mind that what is published might be read by other staff, Governors, pupils, the general public, future employers and friends and family for a long time.
- Ensure that their on-line profiles are consistent with the professional image expected by us and should not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct which may be dealt with under the school's disciplinary procedure. Even where it is made clear that the writer's views on such topics do not represent those of the school, such comments are inappropriate.
- Disclose any information confidential to the school to third parties
- Publish material that is illegal
- Restrict access to certain groups of people on their social media sites and pages.
- Link to your own blog or other personal web pages to the school website

Those working with children have a legal duty of care and are therefore, expected to adopt the highest standards of behaviour to retain the confidence and respect of governors, colleagues and pupils both within and outside of the school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties e.g. for 'cyber-bullying' or identity theft.

Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality.

Staff should keep any communications with pupils transparent and professional and should only use the School's systems for communications. Governors should be mindful of this as well and act similarly in the course of their duties.

If there is any doubt or uncertainty about whether communication between a pupil/ parent and member of staff is acceptable and appropriate a member of the School's leadership team should be informed; so that they can decide how to deal with the situation. All staff are personally responsible for what they communicate on social media.

Often materials published will be accessible by the public and will remain accessible for a long time. Before joining the School, new employees should check any information they have posted on social media sites and remove any post(s) that could embarrassment or offence.

6.5 Misuse of Social Media

While acknowledging the undoubted benefits of social media and the internet; it is also important to recognise that there is a risk to the safety and well-being of users. This is ever-changing and evolving and that the misuse/abuse of these facilities can range from inappropriate to criminal. Misuse of social media can be summarised as follows:

Contact

- Commercial (tracking, harvesting personal information).
- Aggressive (being bullied, harassed or stalked).
- Sexual (meeting strangers, being groomed).
- Values (self-harm, unwelcome persuasions).

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams).
- Aggressive (bullying or harassing another).
- Sexual (creating and uploading inappropriate material).
- Values (providing misleading information or advice).

Content

- Commercial (adverts, spam, sponsorship, personal information).
- Aggressive (violent/hateful content).
- Sexual (pornographic or unwelcome sexual content).
- Values (bias, any protected characteristic defined under the Equality Act 2010, misleading info or advice).

6.6. Misconduct and Disciplinary Action

Any alleged breach of conduct under this policy may lead to disciplinary action under the school's disciplinary policy and procedure. Any serious breaches of this policy which are proven, such as incidents of bullying or of social media activity causing reputational or material damage to the school, may constitute gross misconduct and could lead to the staff member's dismissal.

In addition all school staff, governors and volunteers must be aware of what is considered to be 'criminal', constituting an illegal act, when using social media or the internet and electronic communication in general. For example buying or selling stolen goods, cypher bullying, inciting of religious hatred and acts of terrorism, the grooming and harassment of a child or young person. These examples are not exhaustive, and you are act caution and on advice if you are unsure.

There may be other actions in which might result in civil offences being committed and being pursued by other parties e.g. downloading of multimedia which infringes copyright.

Teachers should be mindful that their standards of conduct have to meet the requirements imposed on them by Part Two of the Teachers' Standards.

https://www.gov.uk/government/publications/teachers-standards

6.7 Monitoring and Reviewing

The school will monitor the impact of this policy using logs of reported incidents and the policy and School practices will be reviewed by the governors annually or more regularly if required, in the light of any incidents that have taken place. The school is also mindful of significant new developments in the use of the technologies, or perceived new threats, in response periodically we will seek professional advice to ensure we are responding appropriately.

6.8 Facebook Usage

At Frank Barnes we are aware that many families will use Facebook regardless of whether or not school choose to do so. By setting up a Facebook Page, we hope to establish a controlled, professional presence that allows us to benefit from this social space in many important ways, while still protecting our pupils and staff.

At Frank Barnes we are aware of the importance of protecting our pupils. Before launching our Facebook Page, our SLT and governors have thought through the types of content they want to share with their families and the wider community. Before sharing any information about any student (including pictures, videos, examples of work, etc.) we will ensure we have obtained consent from the member of staff or child's parent or carer. We will not share names of pupils, only class names.

It is also important to note that we are not encouraging or condoning the use of Facebook for under 13s and that our page is for the benefit of their parents and carers. We do however understand that adults may wish to share the news and content with their children, so will do our utmost to ensure that we monitor all content and restrict who can post to or "Like" our page. Any person that we suspect or know to be under 13 will be blocked and we will not allow them to 'like' the page.

Ways that we will use our Facebook Page

School News: Facebook is a great opportunity for our school to connect with families and share information rapidly. We aim to keep the information updated and accurate about what is going on at our school. On our Facebook Page we will post exciting events around the school via a status update that posts on the Page's wall. This is an easy way to keep families informed as to what is going on during the school day. Furthermore, it only takes moments to do. Photos of exciting school events or of children who have worked hard to achieve something, may be shared on the page.

Share Upcoming Events: Our Facebook Page is an excellent opportunity for Frank Barnes to post upcoming events using the Facebook Events app. This app not only allows people to RSVP, but also makes it easy for them to share that they are attending the events. We can update attendees about any change in plans and send out a reminder as the event approaches.

Make School Announcements: For instance, if there is a snow day, or simply children need a reminder to bring their PE kit tomorrow, we will share this on our Facebook Page, the news will be sent to the walls of everyone that has "liked" the page. However, we will continue to use our other forms of communication for important information e.g. home school book, letters etc., as we do not expect everyone to check the Facebook page regularly.

Showcase School Culture: Our school prides itself on creating a unique culture that promotes not only learning but also the social development of its pupils. Our Facebook page provides an opportunity to showcase this unique culture for those who can't be in the building during the school day or who would like to find out more about what we do.

Sharing Photos and Videos: Photos and videos are an accessible and visual way to showcase our school. We may choose to post photos or videos of:

- Celebrations of pupils' work
- School trips
- Assemblies or school-wide celebrations
- Recognition of individual or group achievements or excellence

Use as a Recruitment Tool: Facebook has the potential to help our school attract skilled teachers and school leaders as well as raise the overall level of awareness surrounding the hard work it is doing. By using Facebook, a school can add another layer to their recruitment efforts and help attract prospective staff and, if applicable, attract pupils as well.

Use Facebook to Attract Pupils: Our school can share the aspects of the school that make it appealing through photos and videos. We may also signpost information, such as how to visit or how to enrol for potential parents or interested professionals.

Get Feedback from our School Community: Facebook allows a school to lower the barriers to participation for members of the community. Our school can make it easier for community members to get involved and share their opinions on a variety of fronts. While some schools may fear this increased participation, we welcome it as the majority of our parents do not live locally to our school and do not have opportunities to have a face-to-face conversation with our parents on a daily basis. We will reserve the right to remove any comments that we feel are detrimental to the values and ethos of our school.

Use Polls: We may choose to use polls to provide a chance for the school to solicit feedback directly from its followers. We can limit the choices available and, with a few simple clicks, everyone who has liked our page will be able to vote. It's a great way to quickly collect data that can help inform decision making.

Settings and Privacy: There are currently only 2 members of staff with administrator rights to the Facebook page. This may be extended to 4 members of staff so that there can be a rota for managing and monitoring of the page. Members of staff may choose to "like" the page but must set up a second "professional" account, so that parents and others that have liked the page cannot see any personal information or images on their personal pages.

Postings: Permissions have been set up with regard to postings on our page:

Only the Facebook page administrator can upload information, pictures and videos.

Those that have "liked" the page cannot add any photo or video content.

Those that have "liked" the page are able to add comments to a posting, but we reserve the right to remove any comments that we feel are detrimental to the school

Unlike with personal photos on Facebook, followers will not be able to tag people in the photos that the school uploads to its Facebook Page. This is to protect the privacy and identity of the pupils

There is a "strong" profanity blocklist in place on our page. If a user attempts to use one of the words on our blocklist (which we can update as necessary) it will automatically be blocked and will not show up on the Facebook page to anyone other than the person who posted the comment and the Facebook administrator , who can then remove it completely and if necessary, block the user.

Our administrator will automatically receive an email when someone has posted to the page to enable constant supervision.

Staff and parents must give permission before their photos are posted on the page.

8. Document Control

Date Approved	Summer 2020

7.0 APPENDICES

Appendix A

Guidance on Responding to Misuse Incidents

Facebook Instagram, Pinterest, Vine or other similar channels (for incidents of cyberbullying or inappropriate behaviour)

- If you know the identity of the perpetrator, contact their parents or, in the case of older children, the young person themselves to ask that the offending content be removed.
- Failing that, having kept a copy of the page or message in question, delete the content and take action as appropriate.
- For messages, on Facebook the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
- For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column.
    - Always try to cite which of the Facebook terms and conditions have been violated at http://www.facebook.com/terms.php or community standards at http://www.facebook.com/communitystandards/

- If the page is authored by someone under 13 years of age then click on the following link: http://www.facebook.com/help/contact.php?show_form=underage .
- To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
- To report abuse or harassment, email abuse@facebook.com. Facebook will acknowledge receipt of your email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint.
- If all else fails, support the victim, if they wish, to contact CEOP' (Child Exploitation & Online Protection Centre) http://www.ceop.police.uk/safety-centre/
- If the person subject of the alleged abuse is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be undertaken via https://ssl.facebook.com/help/contact.php?show_form=delete_account.
- They should be made aware of the privacy issues that might have given rise to their problem in the first place:
    - You will not bully, intimidate, or harass any user.
    - You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
    - You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.

The school's policies and protocols on child protection, safeguarding and online safety **must** be followed and complied with if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

- Any actions online that impact on the school and can potentially damage the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will **always** be responded to.

- In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites professional advice will be sought by the school. Possible outcomes are that the police will be involved and/or legal action pursued by the school and/or disciplinary action may result.

- The current Criminal Prosecution Service (CPS) guidance 'Guidelines on prosecuting cases involving communications sent via social media' came into effect on 20 June 2013 and set out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media.

Appendix B

Acceptable use policy for primary school pupils

Name: **Class:**

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 my password 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
- only email people I know or if my teacher agrees
- only use my school email address
- talk to my teacher before using anything on the internet
- not tell people about myself on-line (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.

Parents

□ I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.

□ I agree that my child's work can be published on the school website.

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:

Date:

Appendix C

Acceptable use policy for staff and governors

Access and professional use

- *All computer networks and systems belong to the school and are made available to staff and governors for educational, professional, administrative and governance purposes only.*
- *Staff and governors are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or governors being removed.*
- *The school reserves the right to monitor internet activity and examine and delete files from the school's system.*
- *Staff and governors have a responsibility to safeguard pupils in their use of the internet and reporting all online safety concerns to the online safety contact officer.*
- *Copyright and intellectual property rights in relation to materials used from the internet must be respected.*
- *E-mails and other written communications must be carefully written and polite in tone and nature.*
- *Anonymous messages and the forwarding of chain letters are not permitted.*
- *Staff and governors will have access to the internet as agreed by the school but will take care not to allow pupils to use their logon to search the internet.*
- *Staff and governors will follow good practice advice at all times and will ensure online activity meets the standards expected of professional conduct.*

Data protection and system security

- *Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.*
- *Use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented on the school ICT system using anti-virus software.*
- *Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.*
- *Staff and governors will not allow others to access their individual accounts. Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.*
- *Files should be saved, stored and deleted in line with the school policy.*
- *Care will be taken to check copyright and not publish or distribute others' work without seeking permission.*

Personal use

- *Staff and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.*
- *Staff and governors should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.*
- *Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.*

- *School ICT systems may not be used for private purposes without permission from the head teacher.*

- *Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.*

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

Print name: _____ ***Sign:*** _____

Line Manager: _____ ***Sign:*** _____

Date: _____

Appendix D

Online safety incident report form

This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

School/organisation's details:

Name of school/organisation:

Address:

Name of online safety co-ordinator:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?

□ In school/service setting □ Outside school/service setting

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify

Type of incident:

□ bullying or harassment (cyber bullying

□ deliberately bypassing security or access

□ hacking or virus propagation

□ racist, sexist, homophobic religious hate material

□ terrorist material

□ online grooming

□ online radicalisation

□ drug/bomb making material

□ child abuse images

□ on-line gambling

□ soft core pornographic material

□ illegal hard core pornographic material

□ other (please specify)

Description of incident

Nature of incident

Deliberate access

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyber bullying □ breach of AUP

Accidental access

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Action taken

Staff

□ incident reported to head teacher/senior manager

□ advice sought from LADO

□ referral made to LADO

□ incident reported to police

□ incident reported to Internet Watch Foundation

□ incident reported to IT

□ disciplinary action to be taken

□ online safety policy to be reviewed/amended

Please detail any specific action taken (i.e.: removal of equipment)

Child/young person

□ incident reported to head teacher/senior manager

□ advice sought from Family Services and Social Work

□ referral made to Family Services and Social Work

□ incident reported to police

□ incident reported to social networking site

□ incident reported to IT

□ child's parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ online safety policy to be reviewed/amended

Appendix E

Outcome of incident/investigation

Description of ICT applications

Technology/ Application	Description/ Usage	Benefits	Risks
Internet	• Enables the storage, publication and retrieval of a vast range of information • Supports communications systems	• Provides access to a wide range of educational materials, information and resources to support learning • Enables pupils and staff to communicate widely with others • Enhances schools management information and business administration systems.	• Information is predominantly for an adult audience and may be unsuitable for children • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.
Email	• Allows written communications over the network and the ability to attach documents.	• Enables exchange of information and ideas and supports collaborative working. • Enhances written communications skills • A good form of communication for children with some disabilities.	• Difficulties controlling contacts and content • Use as a platform for bullying and harassment • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems • Hacking • Unsolicited mail.
Chat/instant messaging/ gaming	• Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people; • Instant messaging allows real-time chat for 2 or more people privately with no-one else able to join. Users have control over who they contact through "buddy lists".	• Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers. • Use of pseudonyms protects the child's identity. • Moderated chat rooms can offer some protection to children.	• Anonymity means that children are not aware of who they are really talking to. • Chat rooms may be used by predatory adults to contact, groom and abuse children on-line. • Risk of children giving away personal information that may identify or locate them. • May be used as a platform to bully or harass.
Social networking sites	• On-line communities, including blogs and podcasts,	• Allows children to network with peers and join forums to	• Open access means children are at risk of unsuitable contact.

	where users can share text, photos and music with others by posting items onto the site and through messaging. • It allows creation of individual profiles. • Users can develop friends lists to allow access to individual profiles and invite comment.	exchange ideas and resources. • It provides a creative outlet and improves ICT skills.	• Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress. • Children may post personal information that allows them to be contacted or located. • May be used as a platform to bully or harass.
File sharing (peer-to- peer networking)	• Allows users to share computer capability, networks and file storage. • Used to share music, video and other materials.	• Allows children to network within a community of peers with similar interests and exchange materials.	• Illegal download and copyright infringement. • Exposure to unsuitable or illegal materials. • Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email.	• Provide children with a good means of communication and entertainment. • They can also keep children safe and allow them to be contacted or stay in contact.	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. • Risk from violent crime due to theft. • Risk of cyberbullying via mobile phones.

Learn, grow and flourish

Frank Barnes
School for Deaf Children

4 Wollstonecraft Street
London
N1C 4BT
www.fbarnes.camden.sch.uk

Tel: 020 7391 7040
SMS: 07970 626 197
Fax: 020 7391 7048
admin@fbarnes.camden.sch.uk