Online Safety Policy

Callis Grange Nursery and Infant School

Amended:	**Term 2 2018 - 2019**
Approved by the Governing Body	**Term 2 2018 – 2019**
Review:	**Term 2 2019 - 2020**

Chair of Governors (Safeguarding Governor): Mr S Beale Date: 12.11.18

Headteacher (Designated Safeguarding Lead): Mrs A Marshall Date: 12.11.18

Deputy Designated Safeguarding Leads: Miss K Shuttle and Miss V Palmer

This is a core policy that forms part of the induction for all staff. It is a requirement that all staff have access to the policy and sign to say that they have read and understood its contents.
This policy will be reviewed annually and/or following any updates to national and local guidance and procedures.

CONTENTS

Introduction

This document was developed through a process of consultation with the Headteacher, teaching staff and the Governors (including parent governors). The review has taken into account the LA specialist guidance and advice as required.

The following DfE statutory guidance documents were used as part of the review:

- 'Keeping Children Safe in Education' (KCSIE) 2018
- Early Years and Foundation Stage 2017
- Working together to Safeguard children 2018 and the
- Kent Safeguarding Children Board procedures.

This policy will be reviewed annually according to the Strategic Plan or following any local or national guidance or legislation changes.

Our Designated Safeguarding Lead (DSL) is the Headteacher Mrs A Marshall. The DSL works closely with the Deputy Designated Safeguarding Leads (DDSL), Miss Shuttle and Miss Palmer, as well as the Computing Subject Leader Miss Russell.

This policy applies to:-

* all staff including teachers, support staff, the governing body, parents, pupils, external visitors and other individuals who work for or provide services on behalf of the school.

* any access to the internet, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off site, such as teacher laptops, tablets or mobile phones.

* other relevant school policies including the Child Protection Policy, Anti-bullying Policy, Behaviour Policy, PSHE Policy and Computing Policy.

What is Online Safety?

Online Safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, *both in and out of school*. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Online Safety is not about restricting children, but educating them, so they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

Online Safety and the Computing Curriculum

Online safety is taught within our Computing Curriculum through Digital Literacy and in every subject within the curriculum whenever our pupils are using the internet. Online safety is also included within our Personal, Social, and Health Education (PSHE) curriculum. Using the "SMART" rules:–

SAFE, MEETING, ACCEPTING, RELIABLE and TELL.

Useful Links:-
www.thinkuknow.co.uk
www.bbc.co.uk/webwise

www.kidsmart.org.uk
www.childnet.com
Online safety rules are displayed in all classrooms/areas where there are computers in use and are discussed with the children regularly.

Why is Online Safety important?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children and adults in danger. At Callis, we are aware that children and staff cannot be prevented from being exposed to risks on or offline. Children should be empowered and educated to manage risk so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. As highlighted by the Ofsted 'Inspecting safeguarding in early years, education and skills settings' (2018):-

"Adults understand the risks posed by adults or learners, who use technology, including the internet, to bully, groom, radicalise or abuse children or learners. They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe".

Aims

At Callis Grange:-

* there is a clear duty to ensure that all children and staff are protected from potential harm online.

* we believe that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

* we know that the internet and information communication technologies are now an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Security and Management of Information Systems

* The security of our school information systems and users will be reviewed regularly by our IT Technician.

* Regular checks will be held on file within our network

* Our school server is located securely, kept up to date and physical access is restricted.

* Virus protection will be updated regularly.

* Personal data taken 'off site' is encrypted.

* User logins and passwords to access the school network are enforced.

* Unapproved software will not be allowed in school or attached to e-mail.

* Portable media may not be used without specific permission followed by an anti-virus scan.

* Staff will not share passwords, leave it where others can find it, or log in as another user at any time.

* All users are expected to log off or lock screens if systems are unattended.

* All staff have their own unique usernames and private passwords to access school systems/laptops.

* Staff family members at no time must use teacher laptops.

* In May 2018, the school adopted an updated Data Protection (GDPR) Policy to ensure that all personal data is dealt with in accordance with the General data Protection Regulation.

Governing Body Key Responsibilities

***** To ensure 'children are taught about safeguarding including online, through teaching and learning opportunities as part of providing a broad and balanced curriculum.' (KCSIE) 2016

* To ensure the school has 'appropriate filters and monitoring systems in place'. (KCSIE) 2016

At Callis Grange online safety forms part of the Governing Body's safeguarding monitoring, undertaken by the Strategy Group. This forms part of the Annual Calendar of Works. An Online Safety Audit is completed annually and presented to the full Governing Body.

Senior Leadership Team Key Responsibilities

* To develop, own and promote the online safety vision and culture to all stakeholders in line with national and local best practice recommendations and requirements with appropriate support and consultation throughout the school community.

* To ensure there are appropriate and up to date policies regarding online safety; including a staff code of conduct (Safe Working Practice at Callis Grange Nursery and infant School) and Acceptable Use Policy.

* To evaluate current online safety practice to identify strengths and areas for improvement.

* To support and work alongside the DDSLs, Miss Shuttle and Miss Palmer, and the Computing Subject Leader, Miss Russell, in the development of an online safety culture within the setting.

* To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensure that the filtering and school network system is actively monitored.

* To ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

* To ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

* To make appropriate resources available to support the development of an online safety culture.

* To take responsibility for online safety incidents and liaise with external agencies as appropriate.
* To ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
* To work with and support technical staff in monitoring the safety and security of schools systems and networks.

Designated Safeguarding Lead (DSL) Key Responsibilities

* To act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate.
* Work alongside the Deputy Designated Safeguarding Leads to ensure online safety is recognised as part of the schools safeguarding responsibilities.
* To keep up-to-date with current research, legislation and trends.
* To liaise with the IT Technician and monitor usage by staff in all areas.
* To ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
* To review and update the Online Safety Policy and Acceptable Use Policy (AUP).
* To ensure that online safety is integrated with other appropriate school policies and procedures.
* To maintain a record of online safety concerns/incidents and actions.
* To ensure that all members of staff are made aware that their online conduct out of school could have an impact on their role and reputation within school (Cross ref: ‘Safe Working Practice at Callis Grange Nursery and Infant School’).
* To ensure all staff receive regular, up-to-date and appropriate online safety training.

All Staff Key Responsibilities

* To contribute to the development of online safety policies.
* To read and sign in agreement of the school ‘Safe working Practice at Callis Grange Nursery and Infant School’ and adhere to it.
* To read and sign in agreement of the school AUP and adhere to it.
* To take responsibility for the security of the school systems and data.
* To have an awareness of online safety issues, and how they relate to the children in their care.
* To model good practice in using new and emerging technologies and demonstrate an emphasis on positive learning opportunities rather than focusing on negatives.
* To embed online safety education in curriculum delivery wherever possible.
* To identify individuals of concern and take appropriate action by working with the DSL/DDSL.
* To know when and how to escalate online safety issues, internally and externally.
* To maintain a professional level of conduct in personal use of technology, both within and outside school.
* To supervise all our pupils when using the internet, teaching them how to use age appropriate tools to research with online.

Technical Support Key Responsibilities

* To provide a safe and secure technical infrastructure which supports safe online practices whilst ensuring that learning opportunities are still maximised.
* To take responsibility for the implementation of safe security of systems and data in partnership with the DSL.
* To ensure that suitable access controls / encryption are implemented to protect personal and sensitive information held on school-owned devices. (All laptops/pen drives are encrypted).
* To ensure that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL and Computing Subject Leader.
* To ensure that the use of the schools network is regularly monitored in order that any deliberate or accidental misuse can be reported to the DSL/DDSL.
* To develop an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
* To ensure that appropriate anti-virus software and system updates are installed and maintained on all machines within the setting and portable devices.

  (Our school server is located securely and physical access is restricted).

Pupils' Key Responsibilities

* To take responsibility for keeping themselves and others safe online.
* To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
* To assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks.
* To be aware of our online safety rules - these are displayed in every classroom. ('Rules to Stay Safe online').
* To respect the feelings and rights of others both on and offline.
* To seek help from a trusted adult if things go wrong.

Our pupils will be taught to tell an adult if they have any concerns and close the laptop/tablet lid.

Parent/Carers Key Responsibilities

* To read and sign in agreement of the school AUP and adhere to it.
* To discuss online safety issues with their children, supporting the school in its online safety approaches, and reinforcing appropriate safe online behaviours at home.
* To role model safe and appropriate uses of new and emerging technology.
* To identify changes in behaviour that could indicate that their child is at risk of harm online.
* To seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns (Cross reference School Website for support agencies).

Enlisting Parents' Support

* Parents/ carers attention will be drawn to the schools' Online Safety Policy and will be regularly informed with regards to online safety issues and safeguarding children online via:

- School Website - CEOP (Child Exploitation and Online Protection) link, Online Safety Tips, PEGI (Pan European Game Information Labels).
- School Newsletters
- Useful Curriculum Websites and Apps Booklet (on our school website and this is sent out each year to parents).

Managing the Safety of the School Website

* Our school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

* The contact details on the website will be the school address, office e-mail and telephone number. Staff or pupils' personal information will not be published.

* The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

* Our school will post information about safeguarding, including online safety on the school website.

* The CEOP (Child Exploitation and Online Protection) link is on our website.

Publishing Pupils' Images/Videos

* Written permission from parents/ carers must be obtained before images/ videos of pupils are published on the school website. The images/videos will be kept by the school until the image/video is no longer in use (see 'Use of Images of Policy' and 'Data Protection Policy (GDPR)).

* Images or videos that include pupils will be selected carefully.

* Pupils' full names will not be used anywhere on the website, particularly in association with photographs, unless permission is obtained from the parent.

Managing E-mail

* Pupils may only use their class e-mail accounts on the school system under the direction of the Class Teacher.

* Pupils must not reveal their personal details or those of others or arrange to meet anyone.

* Staff will only use the official school office e-mail account to communicate with parents and school provided e-mail accounts for other school business.

* E-mails sent to external organisations should be carefully written and authorised before sending, in the same way as a letter written on school headed paper would be.

* Staff should not use personal e-mail accounts during school hours or for professional purposes.

* Staff should not use their school e-mail account for personal purposes.

Filtering and Monitoring

At Callis Grange **we recognise that no filtering or monitoring solution can offer 100% protection** to safeguard pupils. Effective classroom management and regular education about safe and responsible use is essential.

An Acceptable Use Policy (AUP) is in place and implementation monitored.

Callis Grange takes all reasonable precautions to safeguard children and staff using appropriate filters and monitoring systems:

i. Physical

Pupil access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

Pupils are always directly supervised when using the computers.

ii. Internet and Web access

The school's broadband access includes filtering appropriate to the age and the maturity of our pupils.

All users will be informed that network and internet use will be monitored and that internet traffic can be traced to the individual user.

The school works with the LA and The Schools Broadband Team to ensure that the filtering policy is continually reviewed. The school uses the Light Speed filtering system via EIS, which blocks sites that fall into categories such as pornography, racial hatred, extremism, etc. Any concerns highlighted by EIS monitoring and filtering will be reported directly to the Headteacher.

A weekly monitoring update is received by the Headteacher from EIS which allows for an overview of how the internet is being used.

The Headteacher (DSL) meets on a regular basis with the school IT Technician and Computing Subject Leader to discuss filtering and monitoring outcomes.

Reporting:

Any breaches of filtering should be reported to the DSL, who will then record the incident and escalate the concern as appropriate.

Any staff or pupil who discovers an unsuitable site must report it to the DSL, who will then record the incident and escalate the concern as appropriate.

The school website includes the CEOP (Child Exploitation and Online Protection) link for immediate reporting.

Any material that the school believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation (IWF), Kent Police or CEOP.

Reducing Online Risks

Callis Grange recognises that the internet is a constantly changing environment with new apps, devices, websites and materials emerging at a rapid pace. Therefore:

* There is appropriate and up-to-date staff training which takes place in a variety of formats.

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer/device. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from internet access.

* A clear mobile phone policy is in place and displayed throughout the school. (Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications).

* Pupils are not permitted to have mobile phones on site.

* Our school will monitor and audit ICT use to establish if the Online Safety Policy is appropriate and that its implementation is effective.

* The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

Managing Personal Data Online

* Personal data will be recorded, processed, transferred and made available according to The General Data Protection Regulation (GDPR) (May 2018) (See Data Protection Policy (GDPR)).

Responding to Online Incidents and Safeguarding Concerns including Radicalisation and Extremism

* Callis Grange adheres to the guidance provided by the LA when responding to an incident or concern.

* The DSL will record all reported incidents and actions taken, e.g. bullying or child protection.

* The DSL will be informed of any online safety incidents involving child protection concerns, which will then be recorded.

* The DSL will ensure that online safety issues are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board procedures.

* The school will inform parents/carers of any incidents or concerns as and when required.

* Where there is cause for concern or fear that illegal activity has or is taking place, the school will contact Kent’s Education Safeguarding Team and escalate the concern to the police.

* If there is a concern that a member of staff may be at risk of radicalisation online, the Headteacher (DSL) will be informed immediately and action taken in line with the Child Protection Policy and Safeguarding Procedures for Managing Allegations Against Staff Policy.

* If there is a concern that a child or parent may be at risk of radicalisation online, the Headteacher (DSL) will be informed immediately, and action taken in line with the Child Protection Policy.

* Complaints about internet misuse will be dealt with by the school’s Complaints procedure.

* All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures regarding concerns.

* Any complaint about staff misuse must be referred to the Headteacher (DSL).

* Any issues (including sanctions) will be dealt with according to the school’s Staff Discipline and Conduct Policy and Procedure, Behaviour Policy and Child Protection Policy.

* All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any school staff or members of the wider school community.

* All online safety complaints and incidents will be recorded, including actions taken.

Online Child Sexual Abuse and Exploitation (including Child Criminal Exploitation)

* The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

* Callis Grange recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or DDSLs).

* The school will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

* The school will ensure that all members of the school community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

* The school will ensure that the ‘Click CEOP’ report button is visible and available to learners and other members of the school community.

* If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

    - Act in accordance with the school's Child Protection Policy and the relevant Kent Safeguarding Children Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to the Front Door Service (if required/appropriate) and immediately inform Kent Police via 101 or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of the pupils involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for pupils, such as offering pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented. The school's Leadership Team will review and update any procedures, where necessary.

- The school will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on the school site or using a setting provided or personal equipment.

- If it is unclear whether a criminal offence has been committed, the DSL (or DDSLs) will obtain advice immediately through Kent's Education Safeguarding Team and/or Kent Police.

- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or DDSLs).

- If pupils at other settings are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or Kent's Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Callis Grange will ensure that all members of the school community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

- The school will respond to concerns regarding IIOC on the school equipment and/or personal equipment, even if access took place off site.

- The school will seek to prevent accidental access to IIOC by using an internet service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL (or DDSLs) will obtain advice immediately through Kent Police and/or Kent's Education Safeguarding Team.

- If made aware of IIOC, the school will:

    - Act in accordance with the school’s Child Protection Policy and the relevant Kent Safeguarding Children Board’s procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent Police or the Local Authority Designated Officer.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, the school will:
    - Ensure that the DSL (or DDSLs) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school-provided devices, the school will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children’s Social Work Service (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Headteacher is informed in line with the school’s Safeguarding Procedures for Managing Allegations Against Staff Policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school’s Safeguarding Procedures for Managing Allegations Against Staff Policy.
    - Quarantine any devices until police advice has been sought.

Cyberbullying (Online Bullying)

Cyberbullying, along with all other forms of bullying, will not be tolerated at Callis Grange. Full details of how the school will respond to cyberbullying are set out in the school’s Anti-Bullying Policy.

Online Hate

Online hate content, directed towards or posted by, specific members of the school community will not be tolerated at Callis Grange and will be responded to in line with existing policies. All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the DSL (or DDSLs) will obtain advice through Kent's Education Safeguarding Team and/or Kent Police.

Management of Kent Learning Zone (KLZ) – Staff and Governor use only

- The IT Technician and DSL will monitor usage by staff and governors in all areas.

- All users will be mindful of copyright issues and will only upload appropriate content onto the KLZ.

- When staff or governors leave the school, their account or rights to specific areas will be disabled.

Management of Mobile Phones and Personal Devices

- Due to the age of the school's pupils they are not allowed to use mobile phones in school or bring them to school. If this is breached, the phone or device will be confiscated and released to parents.

- Visitors to school are asked to turn off or put mobile phones to silent and not use on site.

- In order that teaching and learning are not impeded, it is school policy that staff mobile phones are not in use on the school site.

- Staff are not permitted to use their own personal phones or devices for contacting pupils or parents within or outside the school in a professional capacity.

- Staff should not use personal devices such as a mobile phones or cameras to take photos or videos of pupils.

- Staff, parents and volunteers on educational visits should not use personal devices such as mobile phones or cameras to take photos or videos of pupils.

- Use of mobile phones and personal devices by parents/carers to take photos or video recordings of pupils at Callis, which include other pupils or staff, must adhere to the school's 'Use of Images Policy'. Parents are asked to sign their agreement to this on their child's entry to school. This agreement remains on their child's file until the child leaves the school. It is the parent's responsibility to notify the school of any change to this agreement.

Pupils Use of Social Media

- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the Acceptable Use Policy (AUP) and taught as part of the curriculum. The pupils' AUP is displayed in all classrooms.

- Pupils will be taught to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile phone numbers, school attended, full names of friends/family, specific interests and clubs etc.

* Pupils will be taught not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

* Pupils will be taught about appropriate security on social media sites and encouraged to use safe passwords and deny access to unknown individuals.

* The school is aware that many popular social media sites state that they are not for children under the age of 13. Therefore, the school will not create accounts within school specifically for children under this age.

* Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

Staff Safe and Responsible Use of Social Networking, Social Media and Personal Publishing Sites

* The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all staff as part of staff induction and will be revisited and communicated via regular staff training opportunities/ information sharing.

* Safe and professional behaviour is outlined for all staff (including volunteers) as part of the school AUP and in the 'Safe Working Practice at Callis Grange Nursery and Infant School'.

* All members of staff should not communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this should be discussed with the DSL (Headteacher).

* All communication between staff and members of the school community on school business will take place via officially-approved communication channels.

* Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

* Any communication from pupils/parents received on personal social media accounts should be reported to the schools DSL (Headteacher).

* Information and contact that staff have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. should not be shared or discussed on personal social media sites.

* All staff are strongly advised to safeguard themselves and their privacy when using social media sites. Staff should be aware of location sharing services, setting the privacy levels of personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

- All staff should carefully consider the information, including text and images, they share and post online and ensure that their social media use is compatible with their professional role and is in accordance with school policies (Child Protection, Confidentiality, Use of Images, Data Protection (GDPR), Online Safety etc.) and the wider professional and legal framework.

- Staff must notify the Headteacher if they consider that any content shared or posted via any information and communications technology including e-mails or social networking sites conflicts with their role in the school.

- Staff should not identify themselves as employees of Callis Grange Nursery and Infant School on their personal social networking accounts.

Continuing Professional Development

- Online safety training for new staff will take place as part of the school's staff induction procedure.

- Online safety updates for staff will take place alongside the school's safeguarding (child protection) training as required.

- Updates will also take place as part of the review of this policy.

Useful Links

Kent Support and Guidance for Educational Settings

Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, Online Safety Development Officer
  - Tel: 03000 415797
- Guidance for Educational Settings:
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - Kent Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk