Online-Safety / Acceptable Use Policy

Bonner Primary School

Key People and Dates

Designated Safeguarding Lead (DSL) team	Nicola Denton Eleanor Ross Anne Mills Louise Havard
ICT Coordinator	Sophia Atherton
PSHE Coordinators	Ryan Kirkpatrick Oliver Larkin
Network manager / Technician	John Sealy / Jon Hime
Approved by:	
Last reviewed on: **October 2018**	
Next review due by: **October 2019**	

Introduction

What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with **'Keeping Children Safe in Education' 2018 (KCSIE)** and other statutory documents; it is designed to sit alongside this school's statutory **Safeguarding Policy**. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

The **LGfL DigiSafe 2018** pupil survey of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

How will this policy be communicated?

This policy can only impact upon practice if it is a regularly updated living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

• Posted on the school website

• Available on the internal staff network

• Available in paper format in the Main Offices on both sites

• Integral to safeguarding updates and training for all staff

• Clearly reflected in the **Acceptable Use Policies (AUPs)** for staff, volunteers, contractors, governors, pupils and parents / carers

• eSafety Policies issued to the whole school community, on **entry** to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review

• Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Scope

This policy applies to all members of the Bonner Primary School community (including staff, governors, volunteers, contractors, pupils, parents / carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Aims

This policy aims to:

• Set out expectations for all Bonner Primary School's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

• Help all stakeholders to recognise that online / digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform

• Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

• Help school staff working with children to understand their roles and responsibilities, to work safely and responsibly with technology and the online world

• Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as our **Behaviour Policy** and our **Anti-Bullying Policy**)

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Head Teacher – Nicola Denton

Key responsibilities:

• Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding

• Ensure that policies and procedures are followed by all staff

• Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant **Local Safeguarding Children Board (LSCB)** guidance

• Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the **Data Protection Officers (DPOs)** and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information

• Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles

• Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

• Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

• Ensure that suitable risk assessments are undertaken so that the curriculum meets the needs of pupils

• Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

• Ensure the school website meets statutory **Department for Education (DfE)** requirements

Designated Safeguarding Lead (DSL) Team

Nicola Denton, Eleanor Ross, Anne Mills, Louise Harvard

Key responsibilities:

The two quotes below are from **'Keeping Children Safe in Education' 2018 (KCSIE)**

"*The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).***"**

"*Liaise with the local authority and work with other agencies in line with* **Working together to safeguard children"**

• Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns

• Work with the **Data Protection Officers (DPOs)** and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information

• Stay up to date with the latest trends in online safety – the new **LGfL DigiSafe Pupil Survey** of 40,000 pupils may be useful reading (new themes include 'self-harm bullying' and getting undressed on camera)

• Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding and others) and submit for review to the governors

• Receive regular updates in online safety issues and legislation, be aware of local and school trends

• Ensure that online safety education is embedded across the curriculum (e.g. by use of the **UK Council for Child Internet Safety (UKCCIS)** framework **'Education for a Connected World'** and beyond, in wider school life

• Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents

• Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident

All staff

Key responsibilities:

• Understand that online safety is a core part of safeguarding; as such it is part of everyone's job

• Know who the **Designated Safeguarding Lead (DSL) Team** are

• Read and follow this policy in conjunction with the school's main **Safeguarding Policy**

• Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.

• To carefully supervise and guide pupils when engaged in learning activities involving online technology supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law

• Encourage pupils to follow the **e-Safety Policy**, remind them about it and enforce school sanctions

• Take a zero-tolerance approach to bullying and low-level sexual harassment (your **DSL** will disseminate relevant information from the new **DfE** document on this)

• Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let a member of the **DSL Team** know

• Receive regular updates from the **DSL** and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the **LGfL DigiSafe Pupil Survey** of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera)

• Model safe, responsible and professional behaviours in pupils' own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this **Online Reputation** guidance for schools

PSHE Coordinators

Ryan Kirkpatrick (Bethnal Green site), Oliver Larkin (Mile End site)

Key responsibilities from September 2019 for September 2020:

The quotes below are taken from the **Department for Education (DfE)** press release on 19 July 2018 on **New relationships and health education in schools**

• As listed in the **'All Staff'** section, plus:

• Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE curriculum, *"complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."*

• Work closely with the **DSL Team** and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE

ICT Coordinator – Sophia Atherton

Key responsibilities:

• As listed in the **'All Staff'** section, plus:

• Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

• Work closely with the **DSL Team** and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

• Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Network Manager / Technician – John Sealy / Jon Hime

Key responsibilities:

• As listed in the **'All Staff'** section, plus:

• Keep up to date with the school's **Online Safety Policy** and technical information in order to effectively carry out their online safety roles and to inform and update others as relevant

• Work closely with the **DSL Team** and **DPOs** to ensure that school systems and networks reflect school policy

• Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the **DSL Team** and Senior Leadership Team (SLT)

• Maintain up-to-date documentation of the school's online security and technical procedures

• To report online-safety related issues that come to their attention in line with school policy

• Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

• Work with the Head Teacher to ensure the school website meets statutory **DfE** requirements (see appendices for website audit document)

• To ensure all **LGfL TRUSTnet** services are managed on behalf of the school in line with school policies, following data handling procedures as relevant

• Understand all existing services and the implications of changes to settings that might be requested – e.g. for YouTube restricted mode, Internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Google G Suite for Education.

• Ensure the **DPOs** are aware of the GDPR information on the relationship between the school and **LGfL TRUSTnet** at gdpr.lgfl.net

Data Protection Officers (DPOs)

Paulette Coulson (Administration), Anne Mills (Curriculum)

Key responsibilities:

• Be aware of references to the relationship between data protection and safeguarding in key **DfE** documents **'Keeping Children Safe in Education'** and **'Data protection: a toolkit for schools' (April 2018)**, especially this quote from the latter document:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding"

The same document states that the retention schedule for safeguarding records may be required to be set as *'Very long-term need (until pupil is aged 25 or older)'*

• Work with the **DSL** and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above

• Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and Contractors

Key responsibilities:

• Read, understand, sign and adhere to an **Acceptable Use Policy (AUP)**

• Report any concerns, no matter how small, to a member of the **Designated Safeguarding Lead (DSL) Team as** named in the **AUP**

• Maintain an awareness of current online safety issues and guidance

• Model safe, responsible and professional behaviours in their own uses of technology

Pupils

Key responsibilities:

• Read, understand and adhere to the **Pupil Acceptable Use Policy**

• Understand the importance of reporting abuse, misuse or access to inappropriate materials

• Know what action to take if they or someone they know feels worried or vulnerable when using online technology

• To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media

• Understand the benefits / opportunities and risks / dangers of the online world and know who to talk to at school or outside school if there are problems

Parents / Carers

Key responsibilities:

• Read and sign the school's **Annual Data Collection Agreement**.

• Consult with the school if they have any concerns about their children's use of technology

• Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents / carers.

Education and Curriculum

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the Internet, new technology such as Augmented Reality, etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, (including extra-curricular and extended school activities), supporting them with search skills, critical thinking, age appropriate materials and legal issues such as copyright and data law. **saferesources.lgfl.net** has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Bonner Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework **'Education for a Connected World'** from **UKCCIS** (the UK Council for Child Internet Safety, soon to become **UKCIS**, no longer solely for children).

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE, Citizenship and (from September 2019 for September 2020) the new statutory **Health Education and Relationships Education**.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to a member of the **DSL Team** to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding Policy
- Child Protection Policy
- Sexual Harassment Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to a member of the **DSL Team** on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern / allegation about staff misuse is always referred directly to the **Head Teacher**, unless the concern is about the **Head Teacher** in which case the matter is referred to the **Chair of Governors** and the **Local Authority's Designated Officer (LADO)**. Staff may also use the **NSPCC Whistleblowing Helpline**.

The school will actively seek support from other agencies as needed (i.e. the **Local Authority, London Grid for Learning (LGFL)**, UK Safer Internet Centre's **Professionals' Online Safety Helpline**, **National Crime Agency (NCA), Child Exploitation and Online Protection command (CEOP)**, **Police, Internet Watch Foundation (IWF)**. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Inappropriate use of the Internet

If an *inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child

• Play the situation down; don't make it into a drama
• Report to the **ICT Coordinator** and decide whether to inform parents of any children who viewed the site
• Inform the school's **ICT Manager / Technician** who will ensure the site is filtered if need be
• Inform **Tower Hamlets Local Authority** if necessary

If an *inappropriate website is accessed <u>intentionally</u> by a child

• Refer to the **Pupil Acceptable Use Policy** and apply agreed sanctions
• Inform a member of the **DSL Team /ICT co-ordinator** and parents of the child.
• Inform the school's **ICT Manager / Technician** who will ensure the site is filtered if need be
• Inform **the GDPR Data Protection Officers (Anne Mills and Paulette Coulson)** if necessary

If an adult uses School IT equipment *inappropriately

• Ensure you have a colleague with you; do not view the misuse alone
• Report the misuse immediately to the **Head Teacher** and ensure that there is no further access to the device
• If the material is offensive, but not illegal, the **Head Teacher** should then:
    • Remove the device to a secure place
    • Identify the precise details of the material
    • Take appropriate disciplinary action
    • Inform governors of the incident
• In an extreme case where the material is of an illegal nature:
    • Contact the Police and follow their advice
    • If requested, to remove the device to a secure place and document what you have done

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff

• Inform and request the comments be removed if the site is administered externally
• Secure and preserve any evidence
• Endeavour to trace the origin and inform the Police as appropriate
• Record the incident in the **Cyber-Bullying Record** held by the Phase Leaders
• Inform the **Local Authority Designated Officer (LADO)**
• The school may wish to consider delivering a parent workshop for the school community

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

• Report to and discuss with a member of the **DSL Team** in school and contact parents
• Consider the involvement of the Police and Social Services
• Advise the child on how to terminate the communication and save all evidence
• Inform the **Local Authority Designated Officer (LADA)**
• Consider delivering a parent workshop for the school community
All of the above incidences must be reported immediately to the **Head Teacher**

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the Internet or mobile technology: they must be able to do this without fear.

***Inappropriate use** includes accessing sites which would be inappropriate for the age of the person accessing it, or the location in which it is accessed. Sites that fall under this definition include but are not limited to: those that promote the use of alcohol, tobacco, gambling, illicit drug use and illegal activities; violence and violent extremist views including acts of extreme cruelty against animals or persons; full or partial nudity, and graphic sex.

Sexting

The school should refer to the **UK Council for Child Internet Safety (UKCCIS)** guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB – where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than a member of the **DSL Team** to first become aware of an incident, and it is vital that the correct steps are taken.

It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Links to the documents referenced above can be found in **Appendices** section at the bottom of this document

Bullying

Online bullying should be treated like any other form of bullying and the **School Anti-Bullying Policy** should be followed for online bullying, which may also be referred to as cyber-bullying.

Sexual Violence and Harassment

In 2018 new **DfE** guidance was issued on sexual violence and harassment, as a new section within **Keeping Children Safe in Education** and also a document in its own right. It would be useful for all staff to be aware of the **DfE** guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to a member of the **DSL Team** who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviour incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Data Protection and Data Security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's **Data Protection Policy** and agreements.

Rigorous controls on the **LGfL TRUSTnet** network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for **LGfL TRUSTnet** services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The **Head Teacher / DPOs** and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first, and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of **USO-FX / Egress** to encrypt all non-internal emails is compulsory for sharing pupil data.

Appropriate Filtering and Monitoring

'Keeping Children Safe in Education' 2018 (**KCSIE)** obliges schools to *"ensure appropriate filters and appropriate monitoring systems are in place* [and] *not be able to access harmful or inappropriate material* [but at the same time] *be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

At this school, the Internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, school-safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 2.0, which is made specifically to protect children in schools.

The **ICT Coordinator** and the school's **ICT Manager / Technician** are able to access these filter settings to ensure they are kept up-to-date. They can limit access to certain websites deemed inappropriate, or those which contain certain key words. Access for pupils can also be limited to a small number of websites between certain times to ensure children are using the Internet appropriately outside of lesson time.

If staff or pupils discover unsuitable sites, the URL must be reported to the **ICT Coordinator**. Any material that the school believes is illegal must be reported to the **Head Teacher**.

You can read more about why this system is appropriate on the **UK Safer Internet Centre's** appropriate filtering submission pages here.

Electronic Communications

Email

• Bonner Primary School knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of **LGfL TRUSTnet** technologies to help protect users and systems in the school, including anti-virus products and other anti-malware products along with direct email filtering for viruses, trojans, pornography, phishing and inappropriate language. Finally, and in support of these, **WebScreen 2.0** filtering monitors and protects our Internet access to the World Wide Web.

• This school does not publish the personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example head@bonner.towerhamlets.sch.uk, for communication with the wider public.

• Pupils at this school use the **LondonMail** system from **LGfL TRUSTnet** for all school emails. These accounts are intentionally 'anonymised' for their protection.

• Children in upper-KS2 may be required to use GoogleMail. Their GoogleMail accounts have been created through G-Suite for Education and are part of the school domain. They have all appropriate safety and security settings enabled.

• Staff at this school use the **StaffMail** system from **LGfL TRUSTnet** for all school emails

• Both these systems are linked to the **Unified Sign On (USO)** authentication system and are fully auditable, trackable and managed by **LGfL TRUSTnet** on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

• Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home.

• Pupils are taught to adhere to the **Pupil Acceptable Use Policy** and to say they have read and understood the online safety rules, including email, and we explain how any inappropriate use will be dealt with.

General principles for email use are as follows:

• Email may only be sent using the email systems above. There should be no circumstances where a private email is used.

• Staff or pupil personal data must never be sent / shared / stored on email.

• If data needs to be shared with external agencies, **USO-FX** and **Egress** systems are available

• Internally, staff should use the school's Intranet, the school's cloud-based Management Information System (MIS) – **RM Integris** and Google's cloud based **G Suite for Education**.

• Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff

• Pupils and staff are **NOT** allowed to use the email systems for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head Teacher and Governors have delegated the day-to-day responsibility of updating the content of the website John Sealy and Jon Hime. The site is managed by and hosted by **London Grid for Learning (LGfL)**

Where pupil work, images or videos are published on the website, their identities are protected and full names are not published. Parents / carers are given a **Pupil Information Form** at the start of the school term which must be returned stating whether they allow or deny permission for their child's image to be included in photographs and videos on the school website.

Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the **DfE** document **'Cloud computing services: guidance for school leaders, school staff and governing bodies'**.

The following principles apply:

• Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud

• The **DPOs** approve new cloud systems, what may or may not be stored in them and by whom. This is noted in a **DPIA (data-protection impact statement)** and parental permission is sought

• Pupils and staff are only given access and / or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen

• Two-factor authentication is used for access to staff or pupil data

• Pupil images / videos are only made public with parental permission

• Only school-approved platforms are used by students or staff to store pupil work

• All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain such as G Suite for Education)

Bonner Primary School currently uses **G Suite for Education** which is a suite of tools that we use to increase opportunities for critical thinking, communication, collaboration, and creativity, all while supporting the learning objectives of the school.

Digital Images and Video

When a pupil joins the school, parents / carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents are asked for their consent for the following:

• Photographs / Videos – for use in school publications

• Photographs / Videos – for use on school website

• Photographs / Videos – for use within school premises

Any pupils shown in public facing materials are never identified with more than first name (and photo file names / tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Bonner Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network or G Suite for Education in line with the retention schedule of the school **Data Protection Policy**.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social media

Bonner Primary School's Social Media presence

Bonner Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Prospective parents will research the school online before making an application.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the **Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk)** involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Anne Mills is responsible for managing our Twitter account. She follows the guidance in the **LGfL / Safer Internet Centre online-reputation management** document here.

Staff, Pupils' and Parents' Social Media presence

Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or teaching profession into disrepute.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's **Safer Internet Strategy**, enforcement and age checking is likely to become more stringent over the coming years.

Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain them to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

It is encouraging that 73% of pupils (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

The school has an official **Twitter** account (managed by Anne Mills) and will respond to general enquiries about the school but asks parents / carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school.

Device usage

Personal devices and bring your own device (BYOD) policy

• Pupils are not allowed to bring mobile phones in to school. Any pupil found with a phone in school will have it confiscated until the end of the school day and the child's parents / carers will be informed. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

• All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the **Digital Images and Video** section on page 22 and **Data Protection and Data Security** section on page 23. Child / staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

• Volunteers, contractors and governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head Teacher should be sought (the Head Teacher may choose to delegate this) and this should be done in the presence of a member staff.

• Parents should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

Network / Internet Access on School Devices

Pupils are not allowed networked file access via personal devices. However, they are allowed to access the school wireless Internet for school-related internet use within the framework of the **Pupil Acceptable Use Policy**. All such use is monitored.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the **Digital Images and Video** section on page 22 and **Data Protection and Data Security** section on page 18. Child and staff data should **never** be downloaded onto a private phone.

Volunteers, contractors and governors can access the wireless network but have no access to networked files/drives, subject to the **Acceptable Use Policy**. All internet traffic is monitored.

Parents have no access to the school network or wireless Internet on personal devices.

School Trips / Events away from school

• **The school provides a mobile phone for School Trips and events out of school hours.** Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Appendices

1. Online-Safety Questions from the Governing Board (UKCCIS)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf

2. Education for a Connected World cross-curricular digital resilience framework (UKCCIS / UKCIS)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

3. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
https://www.saferrecruitmentconsortium.org/GSWP%20Oct%202015.pdf

4. Working together to safeguard children (DfE)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/Working_Together_to_Safeguard_Children-2018.pdf

5. Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719902/Sexual_violence_and_sexual_harassment_between_children_in_schools_and_colleges.pdf

6. Sexting guidance from UKCCIS - Overview for all staff
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf

7. Sexting guidance from UKCCIS - Full guidance for school DSLs
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

8. DfE press release (19 July 2018) – 'New relationships and health education in schools'
https://www.gov.uk/government/news/new-relationships-and-health-education-in-schools

9. Preventing and tackling bullying (DfE)
https://www.gov.uk/government/publications/approaches-to-preventing-and-tackling-bullying

10. Cyber bullying: advice for Head Teachers and school staff (DfE)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf