Ridgeway Primary School and Nursery

Online Safety Policy

Status:	Statutory
Source:	LGFL Template Policy (Cross-referenced with existing school policies)
Last reviewed by:	HST
Approved by:	L&A Committee
Date of approval:	28/1/2020
Frequency of review:	Annually
Date for next review:	Autumn 2021
Published on:	Website / Fronter

Policy is written in conjunction with: Data Protection Policy

Revision date	Section	Significant changes made
21/12/2019		New policy

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	Rebecca Shelley (DSL) Suzanne Kelly (DSO) Jonathan Smith (DSO) Dawn Gibbs (DSO) Rachel Hosking (DSO) Chris Avery (DSO) Cherain Gordon-Todd (DSO)
	Online safety lead (if different)	Jonathan Smith
	Online safety / safeguarding link governor	Craig Rooney
	Computing lead	April Williams
	PSHE/RSHE lead	Sally Kennedy
	Curriculum Network manager / other technical support	Geoff Blyth
	Admin Network manager / other technical support	Octavo Services
	Date this policy was reviewed and by whom	18/12/2019 Jonathan Smith & Heather Armstrong
	Date of next review and by whom	Autumn 2020 Online safety lead

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety related to safeguarding will 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.

Many of these new risks are mentioned in KCSIE 2019 (e.g. fake news and sticky design). To keep yourself updated with prominent new and emerging trends, follow safeblog.lgfl.net. 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 the dangers that can be presented by contact with unknown

people online (i.e. meeting strangers online and then meeting them face to face). 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 or sexual videos, self-harm materials, and 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 document. It must be accessible to, and understood by, all stakeholders. It will be communicated in the following ways:

- Posted on the school website in the **Online Safety** section
- Available for staff on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including non-classroom-based staff)
- 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
- AUPs issued to 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
- AUPs are displayed in appropriate locations (e.g. classrooms)

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all Ridgeway Primary School 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:
    - for the protection and benefit of the children and young people in their care
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- 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 the Behaviour Policy, which includes Anti-Bullying)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to online safety incidents, which should be reported in line with the school's Safeguarding Policy. The DSL will handle referrals to the Croydon Local Authority Single Point of Contact (SPOC) and normally the Headship Team (HST) will handle referrals to the Croydon LA designated officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud. These might be useful for parents and can provide anonymous support for children and young people.

Scope

This policy applies to all members of the Ridgeway 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, or who use technology in their school role.

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.

Co-headteachers

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- 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 Partnerships
- Liaise with the DSL on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL 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 and 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 suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

Designated Safeguarding Lead / Online Safety Lead

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online safety lead, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2019):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety) "
- Where the online safety lead is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate "
- "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 Co-headteachers, DPO 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
- 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, Prevent 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 – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum and 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
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with HST and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring is managed with the Network Manager
- 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 recorded on the Online Safety Incident Log and, if appropriate, the CPOMS system for safeguarding incidents, or the school's Behaviour Log
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

Commented [1]: Should this be 'filter'?

Commented [JS2R1]:

Governing Body, led by Online Safety / Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2019):

- Approve this policy and strategy and subsequently review its effectiveness
- "Ensure an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online safety lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Co-headteachers 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
- Check all school staff have read Part 1 of KCSIE; HST and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three

safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding"
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole-school or college approach to online safety [with] a clear policy on the use of mobile technology"

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for HST and those working directly with children, it is good practice for all staff to read all three sections)
- Read and follow this policy in conjunction with the school's main Safeguarding Policy
- Record online safety incidents by reporting them to the DSL or OSL and, if deemed necessary by the DSL, on CPOMS
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the Staff Acceptable Use Policy and Staff Handbook
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- 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, etc.) in school or setting as home learning tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age-appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), 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
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils to follow their Acceptable Use Policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and peer-on-peer abuse including 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 and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside the school hours and off-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

Well–Being Lead

Key responsibilities:

As listed in the 'all staff' section, plus:

- Embed consent, mental well-being, healthy relationships and staying safe online into the Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives"
- This will complement the Computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within RSE

Computing Lead

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/OSL 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

Subject leaders

Key responsibilities:

As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in their subject, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in their context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Network Manager/technician

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 role and to inform and update others as relevant
- Work closely with the DSL /OSL / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms, etc.)
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and HST
- 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
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO) – SCCGDPR Services

Key responsibilities:

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 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. Lawful 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. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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."

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)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area

- Work with the DSL, Co-headteachers and Admin staff 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

LGfL TRUSTnet Nominated contacts

Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at gdpr.lgfl.net

Volunteers and Contractors

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the DSL / OSL as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil Acceptable Use Policy (AUP) and review this annually with an appropriate school adult (e.g. class teacher)
- 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 AUPs 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, sign and promote the school's parental Acceptable Use Policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' 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 others' 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

External groups including parent associations (e.g. PTCA)

Key responsibilities:

- Any external individual/organisation will sign an Acceptable Use Policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing others' 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

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE (until August 2020)

- Relationships education, relationships and sex education (RSE) and health (from September 2020)
- Computing
- Citizenship

However, as stated in the role descriptors above, 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, supporting subject team leaders, 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 home learning tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age-appropriateness of websites (the Network Manager has details of the web filtering applied by the school).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), 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. Regularly updated theme-based resources, materials and signposting for teachers and parents can be found at: saferesources.lgfl.net.

At Ridgeway Primary School, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum. Online safety will be a key element of our Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum. We will use sources (such as the cross-curricular framework 'Education for a Connected World' from UKCIS) when planning our coverage of online safety.

Annual reviews of curriculum plans (including for SEND pupils) are used as an opportunity to ensure we are covering the key areas of: Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Well-being and lifestyle, Privacy and security, and Copyright and ownership.

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/RSHE and Citizenship).

General concerns must be reported to the DSL or OSL; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the OSL / DSL to contribute to the overall picture or highlight what might not yet be a problem.

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

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Behaviour Policy (including Anti-Bullying Policy)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use, etc.)
- Staff Code of Conduct

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 the OSL /DSL, as soon as possible, but at least on the same day.

Any concern/allegation about staff misuse is always referred directly to the Co-headteachers, unless the concern is about the Co-headteachers, in which case the complaint should be referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, 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.

Actions where there are concerns about a child

Any online safety incident that raises safeguarding will be managed according to the school's Safeguarding procedures and policy.

Bullying

Online bullying should be treated like any other form of bullying and the school Behaviour and Anti-bullying Policy will be followed for online bullying, which may also be referred to as cyberbullying.
Materials to support teaching about bullying and useful DfE guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right ('Sexual violence and sexual harassment between children in schools and colleges'). It would be useful for all staff to be aware of this 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 the DSL 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 behaviours incorrectly viewed as 'low- level' are treated seriously and not allowed to perpetuate.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well-communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the Staff Code of Conduct and Staff Handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Ridgeway Primary School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school Behaviour Policy (for pupils and parents) or Code of Conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Ridgeway Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff:

Commented [3]: I can't see any coloured highlights?

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful 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. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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**."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. Furthermore, this school makes use of the following GDPR solution from LGfL:

- GDPRiS from Groupcall

Rigorous controls on the LGfL 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 services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Malware Bytes, Egress.

The Co-headteachers, data protection officer 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.

Please refer to the school's Data Protection Policy for further information about how we are GDPR compliant.

Appropriate filtering and monitoring

Keeping Children Safe in Education 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. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access monitoring
3. Active/Pro-active technology monitoring services

At Ridgeway Primary School, we use a combination of all three types of monitoring to keep children safe.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, Communication Policy, Staff Code of Conduct and the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils do not currently use email within school. However, if this is introduced to our curriculum, they will use the LondonMail / PupilMail system from LGfL for all school emails
- Staff and governors at this school use the LGfL StaffMail system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL 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.

General principles for email use are as follows:

- Email and Fronter19 are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the Co-headteachers. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the HST (if by a child) or to the DSL or a DSO (if by a staff member)
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Co-headteachers/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately
- Staff or pupil personal data should never be sent/shared/stored on email:
    - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL
    - Internally, staff should use the school network, including when working from home when remote access is available via the Home 2 Office Remote Access system provided by Octavo Partnership
- Pupils in all year groups are restricted to emailing within the school and cannot email external accounts
- 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 system 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

Commented [4]: Does this also relate to governors? If so, this should be made clear

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 Co-headteachers and Governors have delegated the day-to-day responsibility of updating the content of the website to the school office staff. The site is managed / hosted by WEBCreative UK.

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that are requirements are met (see appendices).

Where other staff submit information for the website, they are asked to remember:

- School has the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public domain images that can be used. Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name)

Cloud platforms

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

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The OSL and Network Manager analyse and decide on which systems and procedures to use before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- 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)

Commented [5]: Do we need this if it doesn't apply to our pupils?

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent). Parents are able to amend their permissions and decline consent at any time and must do so in writing. Parents provide permission for the following:

- Name to be used on the school website, printed publications and local media
- Work to be used in school displays and on the school website
- Image to be used within school (for example, in wall-mounted displays and screens)
- Image to be used in books and learning journals as evidence of work completed
- Image to be used in printed school publications (for example, Newsline, school brochures)
- Image to be used on the school website
- Image to be used in the local media
- Image to be taken by the school photographer for individual and sibling photos (we will not be able to include your child in these photographs if consent is not given)
- Image to be taken by the school photographer for whole- class photos (we will not be able to include your child in these photographs if consent is not given)

Whenever a photo or video is taken/made, the member of staff taking it will check the parental permissions before using it for any purpose.

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 Ridgeway 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 in line with the Retention Policy.

Parents/carers can be given permission by a member of the HST to take photographs or videos at specific events. Parents/carers are reminded about the importance of not sharing photographs or videos via any form of media (including social media) due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection).

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make personal information public.

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 / a friend are subject to bullying or abuse.

Social media

Ridgeway Primary School's SM presence

Ridgeway 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). 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 monitor our social media footprint carefully to know what is being said about the school and track and respond to individuals in a fair, responsible manner, even though there are no official/active school social media accounts.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) 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 should adhere to, 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 (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

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, but the school regularly deals with issues arising on social media with pupils under the 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.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. 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 with whom, for how long, and when.

The school uses Fronter19 as a learning platform. It should only be used for matters related to learning.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils and families should not 'follow' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control; this highlights the need for staff to remain professional in their private lives and use of social media. In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Co-headteachers, and should be declared upon entry of the pupil or staff member to the school
** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a staff member) or to the Co-headteachers (if by a child)

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute.

Device usage

Please read the following in conjunction with Acceptable Use Policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** in KS2 are allowed to bring mobile phones in to school, with parental permission, if deemed necessary (for example if they are walking home by themselves). Pupils must hand in their mobile phones to the HST as soon as they arrive at school. Mobile phones must be switched off before being handed in. Pupils may have this privilege withdrawn if they do not adhere to these rules. In the case of emergencies, important messages and phone calls to or from parents can be made at the school

office. Pupils must not use any personal device (including mobile phones, cameras, watches, etc.) to take photographs or video recording anywhere on the school site.

- **All staff who work directly with children** should leave their mobile phones on silent or switched off and ensure they are out of sight during learning time and in learning spaces (e.g. classrooms and corridors). Staff should only use their mobile phones during break times and in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** should leave their phones in their pocket/bag and turned off when they are **on site**. 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 Co-headteachers should be sought (the Co-headteachers may choose to delegate this) and this should be done in the presence of a member of staff.
- **Parents** are asked to leave their phones in their pockets/bag and turned off when they are **on site**. Permission to take photographs and/or videos may only be given by the HST. Any and all photographs and/or videos are for personal viewing only and must not be shared via any method (text, email, social media, etc.)

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 network, using school equipment (e.g. laptops) for school-related internet use within the framework of the Acceptable Use Policy. All such use is monitored
- **Staff** are not permitted to access the school network or wireless internet on personal devices
- **Volunteers, contractors** have no access to the school network or wireless internet on personal devices
- **Governors** can access the guest 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

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number may be used for any authorised or emergency communications with parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Co-headteachers. 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.

The school office will use a central text message and email distribution service to provide parents with any updates about trips as necessary (e.g. an unexpected late return).

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Co-headteachers, and staff authorised by them, have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.