|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Duke Street Primary School |  | Designated Safeguarding Lead (DSL) | | Rachel Von-kaenel  Emma Robinson |
| Safeguarding Governor | | Melissa Abbott |
| PSHE/RSHE lead | | Laura Partington |
| IT Lead | | Natalie Ainsworth |
| Date this policy was reviewed and by whom | | Rachel Von-kaenel  Natalie Ainsworth  August 24 |
| Date of next review and by whom | | Rachel Von-kaenel  Natalie Ainsworth  August 25 |

|  |
| --- |
| **Overview** |
| **Aims** |

This policy aims to:

* Set out expectations for all Duke Street Primary community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
* Help everyone to recognise that online 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, respectful and positive use of technology to support teaching & learning. As well as increasing attainment levels, preparing 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, and 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 violations will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

# Scope

This policy applies to all members of the Duke Street Primary community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/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

Our school is a community and all members have a duty to behave respectfully online and offline. We use technology for teaching and learning across various subjects. Any concerns or inappropriate behaviour needs to be reported immediately, to protect staff, pupils, families and the reputation of the school. We learn together and support each other in a world that is online and offline at the same time.

## Co Headteachers - Andrew Kidd & Sarah Ridley

**Key responsibilities:**

* Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
* Oversee the activities of the designated safeguarding lead 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 designated safeguarding lead 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, 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 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 there is a system in place to monitor and support staff 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.

## Online Safety Lead’s - Rachel Von-kaenel & Emma Robinson

* 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 staff on safeguarding matters when deciding whether to make a referral and liaise with relevant agencies.
* Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
* Work with the Headteacher, DSL’s 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 safeguarding and “undertake Prevent awareness training.
* 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.
* Ensure that online safety education is embedded across the curriculum in line with the statutory

RSHE guidance by use of the updated UKCIS framework.

* Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents especially hard-to-reach parents.
* Communicate regularly with SLT and the safeguarding governor to discuss current issues, review how filtering and monitoring work and have been functioning/helping.
* 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.
* Oversee appropriate filtering and monitoring to keep children safe but “be careful that ‘over blocking’ does not lead to unreasonable restrictions” (KCSIE).
* Ensure the updated Part 5 of Keeping Children Safe in Education is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.

## Governing Body

**Key responsibilities:**

* Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf)
* 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 coordinator/DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
* Work with the Online Safety Lead and headteacher 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; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school

## 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) is and read Part 1, Keeping Children Safe in Education.
* 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.
* 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 code of conduct
* Notify the DSL 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 as part of a whole school approach. Ensuring this is in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise.
* Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
* Be aware of security best-practice at all times, including password hygiene and phishing strategies.
* Prepare and check all online source and resources before using.
* Notify the DSL/OSL of new trends and issues before they become a problem.
* Take a zero-tolerance approach to bullying and sexual harassment.
* Be aware that you are often most likely to see or overhear online-safety issues in the playground, corridors, toilets 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 safeguarding issues
* Model safe, responsible and professional behaviours in their own use of technology. This includes outside of school hours. 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](http://onlinerep.lgfl.net/) guidance for schools.

## Computing Lead – Natalie Ainsworth

Key responsibilities are 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 RSHE lead to avoid overlap but ensure a complementary whole-school approach.
* 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 are as listed in the ‘all staff’ section, plus:

* Look for opportunities to embed online safety in your subject, especially as part of the new RSHE curriculum, 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 your context
* Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
* Ensure subject specific action plans also have an online-safety element

## Pupils

**Key responsibilities:**

* Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
* Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff.
* Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
* To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school.
* Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
* 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:**

* 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, respectful 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

The following subjects have the clearest online safety links:

* Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
* 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 leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology 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, 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.

At Duke Street Primary 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 – 2020 edition’ from UKCIS (the UK Council for Internet Safety).

# Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as all other concerns; safeguarding is often referred to as a jigsaw puzzle, so staff should talk to the online safety lead/designated safeguarding lead to contribute to the overall picture.

Support 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.

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

● Anti-Bullying Policy

● Behaviour 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. 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 violation should be reported to the online safety lead/designated safeguarding lead on the same day – where clearly urgent, it will be made immediately.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is 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, UK Safer Internet Centre’s Professionals’ Online Safety Helpline (POSH), 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 (particular procedures are in place for sexting and upskirting).

## Sexting – sharing nudes and semi-nudes

* All schools should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people) to avoid unnecessary criminalisation of children.
* The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947545/UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_settings_V2.pdf) to decide next steps and whether other agencies need to be involved.
* It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if required.

## Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education. Pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

## Bullying

Online bullying and online child on child abuse should be treated like any other form of bullying and the school bullying policy should be followed.

**Sexual violence and harassment**

DfE guidance on sexual violence and harassment is referenced in part 5 of Keeping Children Safe in Education 22 and It would be useful for all staff to be aware of this guidance.

Any incident of sexual harassment or violence should be reported to the DSL who will follow the full guidance. Staff will 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. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

## 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

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

Social media incidents will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (staff).

Further to this, where an incident relates to an inappropriate social media post by a member of the school community, Duke Street 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, POSH.

# Appropriate filtering and monitoring

Keeping Children Safe in Education 23 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.”

Duke Street Primary School now uses SENSO filtering and monitoring software. This system is managed by Benchmark. The software recognises when a staff or pupil have typed something that may need further investigation. They notify the DSL and SLT who will decide the best course of action to be taken Such as speaking to the child involved.

We have a ‘managed’ system as opposed to a ‘locked down’ system. Members of staff may request websites to be unblocked or specific applications to be downloaded – this is in line with best practice guidelines recommended by the Byron Report and Ofsted. Any request for the unblocking of a website should be made to the Head Teachers. The requester needs to provide a clear reason and teaching/learning benefit for a site to be unblocked. A website or application may be unblocked for a temporary period only.

Antiviral software SENSO is updated regularly to all staff laptops and school PC’s via the network. In the event of a virus on a staff laptop, the member of staff involved must allow prompt action to clear the virus by a technician, and respond positively to their instructions/advice. Should a virus infect any of the staff laptops or school PC’s, a warning message identifying the type of virus and the machine affected will be sent by the server to the Office PC. Mrs Nicholls will monitor and log these virus alerts and pass the information to the ICT Co-ordinator and Technician who will ensure it is rectified as soon as possible. Any user who is alerted to security issues or incidences of inappropriate use must notify the ICT Coordinator, Head Teachers, Online Safeguarding Champion, DSL or member of the SLT immediately, and record it in the Incident Log. The incidences of viruses will be monitored by the ICT Co-ordinator.

# Network management (user access, backup)

This school

* Uses individual, audited log-ins for all users
* Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
* Has additional local network monitoring/auditing software installed;
* Ensures the Systems Administrator/network manager is up-to-date with LA services and policies/requires the Technical Support Provider to be up-to-date with LA services and policies;
* Has regular back-up of school data (admin and curriculum);
* Uses secure, ‘Cloud’ storage for data back-up that conforms to [DfE guidance;](https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act)
* Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive w](http://en.wikipedia.org/wiki/Data_Protection_Directive)here storage is hosted within the EU.

To ensure the network is used safely, this school:

* Ensures staff read and sign that they have understood the school’s Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school’s remote network.
* All pupils have their own unique username and password which gives them access to the Internet and other services;
* Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
* Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
* Requires all users to log off when they have finished working or are leaving the computer unattended;
* Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
* Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
* Maintains equipment to ensure Health and Safety is followed;
* Ensures that access to the school’s network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
* Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
* Has a clear disaster recovery system in place that includes a secure, remote off site back up of data.
* Our wireless network has been secured to industry standard LA security level/appropriate standards suitable for educational use;
* All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;
* This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the subject Leader should be notified immediately.
* All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
* We require staff to use STRONG passwords that include a capital letter and number.
* We require staff to change their passwords every year.

# Email

* Provides staff with an email account for their professional use
* Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
* Will ensure that email accounts are maintained and up to date
* We use a number of LA provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

# School website

The school website is a key public-facing information portal for the school community with a key reputational value. The Headteacher as well as the teaching staff are permitted to update the website on a day to day basis. The DfE has determined information which must be available on a school website.

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

* Schools have 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. If in doubt, check with DLS or OSL.
* Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

# 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.

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

Any pupils shown in public facing materials are never identified with more than first name.

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 Duke Street Primary no member of staff will ever use their personal phone to capture photos or videos of pupils.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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 public, personal information.

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, 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/or a friend are subject to bullying or abuse.

|  |
| --- |
| **Social media** |

Duke Street 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). Few parents will apply for a school place without first ‘googling’ the school, and the Ofsted pre-inspection check includes monitoring what is being said online. 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.

Lorraine Nicholls (Office Manager) is responsible for managing our whole school Facebook and Twitter pages. Lorraine has been trained in effective safe use of social media.

## 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 (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.

Many social media platforms have a minimum age of 13, but the school sometimes 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 the Online Harms Regulation is likely to require more stringent age verification measures 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 peer on peer abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Each class has its own email address and this is the official electronic communication channel between parents and class teachers, any other issues should be directed to the office or headteacher.

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 are discouraged from ‘following’ 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. In the reverse situation, however, staff must not follow such public student accounts.

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, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity.

# Device usage

* Mobile devices brought into school are entirely at that persons own risk The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
* No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be turned off and kept in the school office.
* The Bluetooth or similar function of a mobile device should be switched off at all times.
* Staff Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
* No images or videos should be taken on mobile devices.
* Staff members may use their phones during school break times.
* All visitors are requested to keep their phones on silent.
* The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring.
* If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
* If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at another time.

**Students’ use of personal devices**

* Children are not allowed to bring personal devices into school or on school trips.
* The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
* If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices.

# Staff use of personal devices

* Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
* Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
* If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
* Staff should not connect personal devices to the school’s Wifi.
* If a member of staff breaches the school policy then disciplinary action may be taken.

## Network / internet access on school devices

* **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.
* **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.
* **Parents** have no access to the school network or wireless internet on personal devices but can access the guest but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

## Trips / events away from school

For school trips/events away from school, teachers will be required to take and use their personal phone for any authorised or emergency communications with pupils and parents. 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.

## Security and Data Management

In line with the requirements of the General Data Protection Regulations (GDPR, 2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

Accurate, secure and fairly processed.

Lawfully processed for limited purposes

Processed in accordance with the data subject’s rights

Adequate, relevant and not excessive

Kept no longer than is necessary

Only transferred to others with adequate protection.

Duke Street Primary School holds key information about pupils on the SIMS system.

The Office Manager accesses the data captured on data collection forms.

Key safeguarding incidents records are logged electronically using CPOMS.

Digital files relating to pupils are transferred using CPOMS when a pupil moves to or from another school, including secondary school, then deleted from Duke Street Primary School’s database. Paper files containing sensitive or personal data are shredded once a pupil has left Duke Street Primary School, or when they have been transferred to CPOMS.

Staff must ensure that any personal or sensitive data is disposed of in the appropriate confidential waste bins on the school premises.

Staff are kept informed of current best practices regarding secure data management via staff meetings and updates from the SLT, DSL and Computing Co-ordinator.