# Duke Street Primary School

# E-Safety Policy

## 2020-2021

Contents

## Developing and reviewing this policy.

This policy will be monitored and reviewed by: Rachel Von-kaenel, Emma Robinson and Andrew Kidd. It will be reviewed and updated annually.

Approved by ………………………………… ………..(Head teacher) Date:……………………………..

Approved by ……………………………………………..(Governor) Date: ………………………..

# E-Safety Policy

## 1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users). It should be read in conjunction with the School's policies and relevant legislation for the following areas:

- Computing Policy
- The Lancashire Safeguarding Children Board Online Safeguarding Policy 2017-2019
- Keeping Children Safe in Education 2019
- Teaching Online Safety in School (DFE, June 2019)
- General Data Protection Act 2018
- Duke Street Primary Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Child Protection Policy
- Staff Code of Conduct
- Staff/Governor/Pupil Acceptable Use Policy (AUP)
- Recruitment and Inclusion Procedures – School Self-Evaluation Framework – School Improvement Plan.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safeguarding Policy will help children to develop the skills and awareness to be more aware of and manage potential risks. This includes exposure to extremist views online.

ICT and the Internet offers almost limitless possibilities for fun, communication and learning through online games, social networking sites, music, videos, texting and virtual learning environments, all of which are increasingly more interlinked, powerful, faster, smaller and mobile.

Duke Street, has an important part to play in guiding and advising staff, pupils, parents, carers and the wider school community towards understanding their respective rights and responsibilities relating to ICT in all it's forms, present or future.

Duke Street School encourages its pupils across all year groups to use the Internet at home to access excellent learning resources in order to deepen the skills and knowledge acquired in class. It is vital that we also teach them how to stay safe when doing so. At the same time, pupils need to be aware of the standards of behaviour expected from them as users of ICT and the Internet, plus the consequences to themselves and to others in the School or wider community which might arise from the misuse of ICT and/or the Internet.

In addition, Duke Street School recognises it's role in enabling pupils to develop awareness of their own 'Digital Wellbeing', in a rapidly evolving and increasingly 'connected' world.

Our Online Safeguarding Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

This Policy will be reviewed on an annual basis by Rachel Von-kaenel, or more frequently if deemed necessary, for example in the light of new developments in ICT which have a direct impact on Online Safeguarding issues.

## 2. Duke Street School's vision for Online Safeguarding

As technology changes rapidly, we aim to teach safe, responsible behaviours which can be applied in a range of different online contexts in an age-appropriate manner. Pupils will learn how to evaluate risks when online and how to manage that risk.

Special consideration will be given to vulnerable groups (as identified in the School Safeguarding Policy), in particular those pupils with Special Educational Needs or Disabilities.

Online Safeguarding principles are embedded in our school curriculum and deliver the requirements of the National Curriculum and the EYFS guidelines, Computing (incorporating Online Safeguarding) is taught both as a discrete subject and through other subjects via the National Curriculum and can be categorised into three areas of risk, the 'Three C's':

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

The use of ICT is encouraged in all year groups, both as a teaching aid and a research tool. It allows the children to present their work in a lively, varied, immediate, focused and creative medium. Through the use of online resources, pupils are able to research information to support cross curricular learning and to develop vital skills which are needed to study and work in the twenty-first century. It also enables children with SEND to access the curriculum more effectively, whilst allowing Gifted, Able or Talented pupils to develop and showcase their skills and understanding at a level appropriate to themselves. Pupils across the school are encouraged to work independently at home through a range of education websites. Overall, the use of ICT is an essential tool to raise standards of teaching and learning in Duke Street Primary School, whilst at the same time being a vehicle to provide a broad, balanced and exciting curriculum.

We are striving to develop an environment where pupils and staff are able to use ICT to work at the highest possible level, and are knowledgeable, safe and responsible users of all forms of technology, including the internet, both in school and at home. Therefore, we acknowledge that Online Safeguarding needs not only to be provided for in the school framework of resources but also specifically included in the curriculum at an age-appropriate level from the Foundation Stage upwards. Online Safeguarding issues are addressed through focused theme weeks, assemblies, PSHE, approaches to behaviour management as well as classroom-based sessions. Staff and governors are also kept informed and updated through twilight training sessions and meetings. The school website and social media pages will also provide parents and carers with information on safe use of the internet, and links to other websites about Online Safeguarding.

The Byron Report (2017) and the Ofsted Review of Safe Use of New Technologies (2010) conclude that children are best placed to become safe and responsible users of ICT in an environment where internet access is actively ‘managed’ rather than ‘locked down’. Children who hold a parent’s hand every time they cross the road are safe. However, unless they are taught to cross the road by themselves, they might not learn to do this independently.

A child whose use of the internet is closely monitored at school will not necessarily develop the level of understanding required to use new technologies safely and responsibly in other contexts, including at home.

Within Duke Street Primary School, Staff and Pupils have different levels of access to the internet, for example staff users are able to access sites blocked to pupils, such as YouTube. This allows staff to access useful resources for use in lessons and assemblies.

Online Safeguarding also encompasses the use of mobile communications technology such as via laptops and mobile phones, the appropriate and safe use of ICT equipment such as cameras, how to deal with incidents and the consequences of misuses.

## 3. The role of the school’s Online Safeguarding Champion

- Having responsibility for ensuring the development, maintenance and review of Duke Street Primary School’s Online Safeguarding Policy and associated policies including Acceptable Use Policies.
- Ensuring that the Policy is implemented and that compliance with the Policy is actively monitored.
- Ensuring that all staff are aware of reporting procedures and requirements should an incident occur.
- Ensuring that the Online Safeguarding Log (on CPOMS) is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safeguarding issues and guidance through liaison with LCC Schools’ ICT Team and through advice given by national agencies such as the SWGFL, Child Exploitation and Online Protection Centre (CEOP)
- Providing or arranging Online Safeguarding advice/training for staff and governors.
- Ensuring the Head Teacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the Child Protection Officer/DSL to ensure a co-ordinated approach across relevant teaching areas.

Online Safeguarding Champion is: Rachel Von-kaenel
Our Child Protection Officer / DSL is: Rachel Von-kaenel
Deputy: Emma Robinson

## 4. Policies and practices

This section of the Online Safeguarding Policy sets out Duke Street Primary School’s approach to online safeguarding along with the various procedures to follow in the event of an incident. Please refer to the policies and legislation detailed in the Introduction.

## 4.1 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
- Fairly and lawfully processed
- 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

All data in Duke Street Primary School is kept secure and staff are informed of what they can and can't do with data through the Online Safeguarding Policy and statements in the staff Acceptable Use Policy.

Key information about pupils is stored on the Server using SIMS. The Office Manager, Lorraine Nicholls can access data relating to family circumstances such as the information captured on data collection forms. Key safeguarding incident 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.

iPads are available for use as a teaching and learning resource and for assessment purposes, particularly in the EYFS. Staff are required to make every effort to ensure the physical security of the iPads. iPads allocated for Teacher/TA use are for school use only. Staff are not permitted to install social networking or other applications for personal use.

Staff should not use personal equipment to record or save images and information about pupils.

Staff should follow the schools process when adding photos to social media or the website. They need to check parental consent for each child. They need to take the photo to Lorraine Nicholls and ensure she double checks the child has permissions. Lorraine can then upload the picture after her checks. She is then able to upload the image. Only Lorraine can add photos containing children to the school website or social media.

No photos/videos of children should be stored longer than is needed for curriculum or assessment purposes on the iPads.

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.

## 4.2 Use of mobile devices:

In our school we recognise the use of mobile devices (such as phones, iPads or any digital equipment with access to a camera or the internet) offers a range of opportunities to extend children's learning.
However:

- Staff, students and visitors to school are not permitted to use a mobile phone in the presence of children.
- Pupils are encouraged NOT to bring mobile phones to school. However we understand that on occasion children may need to do so. If this is the case then these children must leave their device switched off and with Mrs Nicholls for the duration of the school day. They can drop off their device prior to 8.55am and collect after 3.15pm. If pupils access Breakfast Club provision then pupils must keep any devices switched off in their bags until the school office opens.
- Mobile devices will be provided by the school for lessons e.g. as an interactive resource, should they decide their use is of educational benefit.
- Mobile phones or other devices can be confiscated if staff believe it is being used to contravene the schools safeguarding, behaviour or bullying policy.
- Confiscated devices can be searched and the contents handed over to Police or other authorities if needed.
- Staff should be vigilant in monitoring for any covert use of mobile phones/cameras, both inside and outside of school. Any concerns should be reported to the SLT. Sanctions many be applied as appropriate and logged using CPOMS.
- Devices such as staff laptops are scanned for viruses when they are connected to the school, server. An alert message indicating the origin and type of virus will be sent to the IT coordinator should they be detected, and action taken as necessary. All computer hardware in school is automatically protected using Sophos anti-viral software.

- All members of staff are aware of best practice regarding keeping their laptops free from viruses, and are kept updated by the IT co-ordinator. When staff log on and off the school network they automatically receive Sophos anti-virus updates. They have read and signed the relevant AUP regarding internet access at home.
- Staff are discouraged from sharing information on memory sticks. Non-sensitive information e.g. planning or lesson resources should be shared amongst staff e-mail using the school e-mail address system.
- All staff have access to a digital camera for use as a teaching and learning resource in school or on school trips only, with key people to ensure the physical security of each device. Staff are NOT allowed to bring their own cameras to use in school.
- Pupils are able to use iPads stored on the portable iPad trolley. This is kept securely in the ICT Suite. Foundation Stage will use their own iPads, ensure they are password protected and kept in a secure place in the classroom.
- Children should save work when appropriate, the iPads will be routinely wiped of stored data (including images) at least annually.

## 4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance. The various forms of digital media used in school such as photographs and videos play an important part in school life as a means of recording children's work as evidence or as a means of showcasing their learning. Children and staff are able to use school equipment such as digital cameras for these purposes, and have opportunities to handle, store and manipulate images of staff and children. Occasions where parents or the wider community are welcomed into school allow opportunities for individuals to record digital images, for personal use only and must not be shared on social media by parents. Parents and visitors to school are reminded of our policy before each event. All photographs and videos of pupils and staff are regarded as personal data in terms of the General Data Protection Act (2018), and before using any images the school obtains written permission from parents and carers.

The following points are taken into consideration:

- Before obtaining or using still or moving images, written consent is sought from staff, parents and carers, on an annual basis using the data collection form.
- Images of a group activity can only be used when all children in the photo have written permission from a parent or carer.
- Images will not normally be retained after a child has left Duke Street Primary School, unless agreement is sought in advance for example for a school archive or historical record.
- Students, or individuals wishing to record evidence for an academic course are not permitted to take photographs of children without prior written permission from the Head Teacher and parents.
- Should any images of pupils be published, for example in a newspaper (paper or online) or on a website, full names or personal details will not be used or appear next to the image, unless parents or carers give their prior, explicit consent.
- Parents and carers who are invited into school for events are allowed to take still or moving images of their own child and use the images for personal use only. Parents and carers are requested not to share or publish the data on the internet or social networking site. Should they include images of any other children in the photo or video, permission should be sought from the other parents before it is uploaded. Parents are also asked to be considerate when taking photographs or videos, and be careful not to obscure the view of other parents, or distract the children, for example during a performance or at a sporting event.
- Children are not allowed to bring cameras, including those on mobile phones, into school.
- Staff are made aware of the potential risks associated with the publication of images, especially with regard to social networking sites through staff meetings and training sessions. They are advised not to publish any images which might compromise their professional standing.
- Still and moving images of pupils undertaken during school activities are taken only using school photographic equipment. Each class have their own equipment, which should not be removed from the school premises, unless with prior permission from a member of the SLT. Images are sometimes stored on

school laptops, which are password protected.  Images must not be stored on memory sticks. Staff are advised not to use or store images on their personal equipment.

- Images taken for school purposes, such as displays, assemblies or lesson resources are to be used by the relevant member of staff only, or in certain circumstances by pupils under supervision, for example to carry out a specific task identified in lesson plans.
- Images of pupils or staff must not be transferred electronically to a destination outside the school network, eg to a personal email account or social networking site. Written consent must be obtained prior to uploading images to a website providing there is a clear link to educational activities on that website, and the names of pupils must not be published near the image in order to avoid the identification of individuals.
- Staff must ensure that when taking still or moving images, pupils are appropriately dressed and not participating in activities which may be misinterpreted. They should not be taken in or near toilets or changing rooms. Any images which appear contrary to this guideline must be deleted immediately.

These guidelines outlining safe practice relating to the use of digital media are to be monitored on an annual basis (or more frequently if the need arises) by Rachel Von-Kaenel.

## 4.4 Communication technologies

All digital communications should be professional in tone and content, using media approved by Duke Street Primary School as described in this Policy.  Only official school e-mail addresses should be used to communicate with staff or parents.

### Email:

All staff have been allocated their personal e-mail address.  Each class also has their own e-mail address, as do particular job functions such as Head or Bursar.  Individual children or groups may be allocated e-mail accounts for specific educational purposes.  Temporary members of staff such as teachers on short term contracts or students on block teaching practice may be allocated accounts if necessary.  The ICT Co-ordinator manages and administers these accounts on a regular basis and ensures accounts are deleted once an individual (staff or pupil) has left Duke Street Primary School.

Staff are advised to use the school email address, (name@dukestreet-pri.lancs.sch.uk) for all professional communications, including regular newsletters from external sources as this system is more secure.  Any incidences of SPAM or e-mails containing unsuitable material should be reported to the IT Coordinator.  Staff have been made aware that there is a greater risk of accessing undesirable content including SPAM, inappropriate pop-ups and viruses by using external e-mail accounts e.g. Hotmail, and have been given advice regarding good practice when sending or receiving e-mails, opening junk mail or clicking on links to other websites.  Internet fraud such as phishing or spyware is increasingly sophisticated and can be costly and time consuming to put right.  Staff will be updated on best, safe practice regularly.

Pupils are taught to send and receive e-mails as one of the requirements of the National Curriculum and will be taught safe practice during ICT lessons in school using online resources. They will also be taught how to safely respond to unsolicited or undesirable email.

Sensitive information, for example a report or communication containing a child’s name must be sent using LCC secure email only.

Pupils or visitors to school are not allowed to use school computers to access external e-mail accounts during or outside school hours.

All users are made aware that e-mail is covered by the General Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

All users are made aware that all e-mail communications may be monitored at any time in accordance with the Acceptable Use Policy.

All users must immediately report any e-mail that makes them feel uncomfortable, is offensive or bullying in nature.

## Social Networks:

Social network sites such as Facebook, Twitter, Snapchat, WhatsApp and Instagram are blocked by Sophos filtering for direct use in Duke Street Primary School by users of the school network. Duke Street Primary School have their own Facebook group, with the aim of informing parents and raising the profile of the school amongst the community. Lorraine Nicholls is the administrator for this page and therefore allowed to upload content. Express permission has been sought from parents to allow images of their children to be posted online.

Comments made on social media sites outside school have the potential to contravene confidentiality, bring the school or staff into disrepute, place pupils and young adults in unsafe situations or at increased risk of cyberbullying. School has a duty of care towards members of staff subjected to online bullying or harassment and can seek legal advice and support to have comments or pages taken down as necessary.
Therefore, Duke Street Primary School's Online Safeguarding Policy also includes guidelines on the use of Social Network sites outside school by staff, pupils, parents and the wider school community. Staff, governors and parents /carers will continue to receive advice and information on safe use of these sites. Pupils will be taught about the risks, potential misuses and safe practice regarding Social Networks though age related curricular activities.

At Duke Street Primary School, the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- Social network sites must not be accessed by anyone in school using either school or their own equipment, unless authorised circumstances.
- Staff must not give personal contact details to pupils, parents or carers, including mobile telephone numbers, or details of any personal blogs or websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If staff are users of Social Network sites, they must ensure privacy settings are at maximum and not share details with pupils.
- Online communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Any inappropriate use, incidences of online bullying or content / comments which are upsetting or controversial and involve any member of staff, pupil or person in the wider community who is associated with Duke Street Primary School must be reported immediately to a member of the SLT, the DSL and the Online Safeguarding Champion. In addition, staff may also wish to contact their respective professional body. Incidents will be logged and appropriate action taken if deemed necessary.
- Pupils will be taught about the potential risks associated with social networking sites and how to use them safely. This includes exposure to extremist and radicalised content. In addition, they will be encouraged to consider the consequences to themselves and others of misuses, and what constitutes cyberbullying or indeed an illegal activity. This includes sexting, upskirting and the sharing of sexual images of themselves or other children under the age of 16, which is illegal.

## Mobile telephones:

As discussed above children are encouraged NOT to bring their mobile phone to school. They are not needed at any time by pupils, and by being brought into Duke Street Primary School the owners run the risk of possible loss, damage or theft.

Pupils will be taught about the potential risks associated with mobile phones, how to use them safely and what action to take if they feel threatened or worried by an incoming call. In addition, they will be encouraged to consider the consequences to themselves and others of misuses, and what constitutes online bullying.

Risk assessments for school trips and the school holiday must include a list of all staff mobile telephone numbers, and group leaders, plus the details of a base contact to ensure swift communication between home, school and any school activity not on the school premises.

If a child is found to have not handed their phone in to Mrs Nicholls at the start of the day then it will be confiscated.

In the event of misuse of a mobile device by a pupil in school or on a school trip, such as to access inappropriate website content, cyberbullying, or the sending of texts which are deemed to be of an inappropriate e.g. sexual nature, the parents of the person or persons held responsible will be informed and the pupil sent home or dealt with as necessary on return to school.

In the event of the misuse of  a mobile device such as a telephone by an adult or member of school staff, the SLT or line manager should be informed and action taken as necessary in accordance with current Safeguarding best practice.

All incidences involving the misuse of mobile communications devices must be reported to the SLT, Online Safeguarding Champion or DSL as appropriate, and actions taken if needed.

Dealing With Incidents.
Incidents must be logged using CPOMS and will be monitored by Rachel Von-kaenel and Emma Robinson.

## Instant Messaging:

Instant messaging e.g. Skype or 'Facetime'  are popular tools for communicating in 'real time' using text, sound and video. These sites are normally blocked on the school network by Sophos Web Filtering system, but can be unblocked with the permission of the Head teacher if needed.

- Staff and children will be made aware of the potential safety risks associated with this type of communication, and of the rules of 'netiquette' before an activity such as an online forum or blog takes place.
- Only children for whom we hold a written permission slip will be permitted to take part.
- Members of staff may request the Head teacher to temporarily unblock these sites, providing they can demonstrate a clear need as a teaching and learning resource.
- Their use will be closely monitored, and restricted to short time periods of access.
- On a regular basis, staff and pupils will use more secure forms of messaging, forum or chat systems via Purple Mash, or other online resources purchased by school. This will monitored by the ICT Co-ordinator and class teacher.
- School keeps records of parent's emails and mobile numbers to communicate important information, such as cancellation of a sporting event. The database is managed by the Lorraine Nicholls and is password protected.

| **Incident** | **Procedure and Sanctions** |
|---|---|
| Accidental access to inappropriate materials | • Minimise the webpage/turn the monitor off<br>• Tell a trusted adult. |

| | |
|---|---|
| | • Enter the details in the Incident Log and report to the filtering services if necessary.<br>• Persistent offenders may need further disciplinary action. |
| Using other people's logins and passwords maliciously. | • Inform SLT or designated E-Safety Champion.<br>• Enter the details in the Incident Log.<br>• Additional awareness raising of E-Safety issues and the AUP with individual child/class.<br>• More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.<br>• Consider parent/carer involvement. |
| Deliberate searching for inappropriate materials. | |
| Bringing inappropriate electronic files from home. | |
| Using chats and forums in an inappropriate way. | |

## Virtual Learning Environment (VLE):

Duke Street Primary School encourage pupils to access learning activities from home via Purple Mash. Class Teachers will be responsible for managing activities on Purple Mash. Pupils will only be able access their own work, and will be issued with their own usernames and passwords in Reception, which will be deleted at the end of Year Six or when they leave Duke Street Primary School. Pupils will be taught the importance of keeping their password safe, and for their personal use only. On occasion, children may be allowed to work collaboratively. The system administrator will have access to all accounts.

Staff have received training and support in the use of Purple Mash, and will have on-going training as needed.

- It is not acceptable to post comments of a personal, sexual, aggressive, insulting, inflammatory, racist, sexist or otherwise threatening nature aimed at either staff, pupils or Duke Street Primary School in general on any area of Purple Mash. It is not acceptable to bring Duke Street Primary School into disrepute.
- Any incidents of unacceptable behaviour will be reported immediately to the class teacher, SLT and Rachel Von-kaenel who will enter it in the Online Safeguarding log.
- Staff /Pupils will be made aware of the correct action to take should they experience any inappropriate material on Purple Mash.

Class Teachers have responsibility for monitoring activity on Purple Mash on a day-to-day basis.

## Web sites and other online publications:

Duke Street Primary School has its own website which acts as a 'showcase' for the school, providing information for parents, pupils and the wider school community. It is accessible to all users of the internet and therefore security issues are paramount. The content is in line with current requirements of the School Information (England) (Amendment) Regulations 2012 and Ofsted guidelines.

Mrs Worth and Mrs Nicholls are responsible for maintaining the website and ensuring content is current, accurate and complies with Duke Street Primary School's Online Safeguarding guidelines regarding personal information and images and that links to other web sites are appropriate and secure. They will also be responsible for checking whether content is subject to copyright/personal intellectual copyright restrictions.

Downloadable materials will be in a PDF or read-only format, to prevent being manipulated and potentially redistributed without the school's consent. Photographic images or video clips including identifiable members of staff or pupils will not be included on the website without their written permission.

Class Teachers are able to upload information to Year Group areas, and must adhere to the Online Safeguarding policy guidelines.

Pupils will be taught the correct action to take should they come across a web page containing inappropriate content. The children will also be taught to alert a member of staff immediately.

## 4.5 Acceptable Use Policy (AUP)

Duke Street Primary School has Acceptable Use Policies which are intended to ensure that all users of technology within school will be responsible and stay safe. They are designed to ensure that all users are protected from potential risk in their everyday day use of ICT for educational, personal and recreational purposes.

There are specific AUP's for Staff, Pupils, Visitors and Guests. The relevant policy/policies must be signed and adhered to by users before access to technology is allowed. AUP's should be seen as a partnership between parents/carers, pupils, Duke Street Primary School and visitors/guests to ensure users are kept safe when using technology, and reflect the technology, procedures and practice at Duke Street Primary School. Signed AUP's for all users are updated annually, or more frequently if needed, and kept in the Main Office.

Visitors and Guests, including other users of Duke Street Primary School must sign them on arrival or annually as required.

The AUP's for Duke Street Primary School are attached to this Online Safeguarding Policy.

## 4.6 Dealing with incidents

Duke Street Primary School has considered the types of incidents that may occur and how these will be dealt with. Any incidents or concerns will be logged on CPOMS immediately by the member of staff concerned and monitored by the DSL.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the DSL/ Head Teacher or LADO as appropriate, who must refer this to external authorities e.g. Police, CEOP, Internet Watch Foundation (IWF).

Staff will be made aware that they must never personally investigate, interfere with, save or share evidence if they come across it as they may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Potential illegal content must always be reported to the Internet Watch Foundation (http://www.iwf.org.uk). They are licensed to investigate – schools are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred
- Incitement to extremism or terrorism *

More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

*School has a duty to 'have due regard to the need to prevent people being drawn into terrorism' (Counter Terrorism and Security Act 2015, s26)

Reporting and Escalation

'Sexting' is now regarded as a common activity by young people under 16.
However, these are actually ILLEGAL images because they are of children. It is also illegal to share these images.

'Upskirting' is also illegal, as is the sharing of any image of this nature.

Reporting Procedure Advice: (All staff) if illegal images of children are reported or suspected, secure or switch off the device and seek advice from DSL about safeguarding procedure. The DSL will look into each incident, determine if it is isolated but almost always should be escalated. Further guidance is available on the CEOP website.

Staff who come across illegal images MUST NOT copy, print ,save or share the image as these actions are also illegal, even if well intentioned!

Inappropriate use

It is more likely that adults in Duke Street Primary School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. The SLT, governors, Online Safeguarding Champion, Computing Coordinator and DSL have what considered what constitutes inappropriate use and the sanctions to be applied. These are listed below in Table 1.

Should an incident occur the school will:

- Immediately refer it to the relevant member of staff - DSL/ SLT or LADO.
- Ensure all staff are aware of the different types of Online Safeguarding incidents and how to respond appropriately.
- Class teachers /TA's will ensure all children are informed of the procedures.
- Incidents will be logged using CPOMS by the appropriate member staff.
- Rachel Von-kaenel and Emma Robinson will monitor the entries on CPOMS regularly.
- Regularly review and amend the measures that are in place to respond to and prevent recurrence of an incident.
- Ensure parents or external agencies are involved, as is deemed necessary by the nature of the incident.

Should an incident occur the school will:

- Immediately refer it to the relevant member of staff either from SLT, Online Safeguarding Champion, ICT coordinator, DSL, or PSHE coordinator.
- Staff are kept aware of the different types of Online Safeguarding incident and how to respond appropriately and that they are sure of the correct procedures to follow.
- All class teachers/TA will ensure all children are informed of the procedures.
- Incidents will be logged in the Inappropriate Use of ICT Logbook
- Regularly review/amend the measures that are in place to respond to and prevent recurrence of an incident.
- Ensure parents or external agencies are involved, as is deemed necessary by the nature of the incident.
- Ensure and regularly review/amend the procedures that are in place to protect staff and escalate a suspected incident/allegation involving a staff member.

## 4.7. Education and training

Both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of Online Safeguarding risk (as mentioned by OFSTED, 2013) that Duke Street Primary School is aware of and considers are:

| Area of Risk | Example of Risk |
|---|---|
| Content:<br>Children need to be taught that not all content is appropriate or from a reliable source. | • Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.<br>• Lifestyle websites or social media influencers, for example with pro-anorexia/self-harm/suicide content.<br>• Hate sites, including those encouraging extreme Right- or Left-Wing views or terrorism.<br>• Content validation: how to check authenticity and accuracy of online content. |
| Contact:<br>Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies. | • Grooming<br>• Online bullying in all forms<br>• Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords. |
| Conduct:<br>Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others. | • Privacy issues, including disclosure of<br>• personal information, digital footprint and<br>• online reputation<br>• Health and well-being - amount of time<br>• spent online (eg social media or gaming, FOMO). • Sexting (sending and receiving of personally<br>• intimate images).<br>• Upskirting (taking images of a person's underwear and genital areas without their knowledge or permission)<br>• Copyright (little care or consideration for •<br>intellectual property and ownership – such • as music and film). |

# 5. Infrastructure and technology

Duke Street Primary School subscribes to the Broadband Service provided by Virtue Technology, which includes Sophos Anti-virus software and web filtering. This provides a secure infrastructure which is also managed via devolved filtering in school in order to provide a system in line with best practice guidelines suggested in the Byron Report (2007) and the Ofsted Review (2010).

Certain categories of website are blocked generically, including shopping, pornography, gaming, social networking and those harbouring extremism or terrorist views.

Pupil Access:

Pupils using computer equipment do so under supervision from a Teacher or TA. They are not allowed to have unsupervised access during the school day e.g. at playtimes.

## Passwords:

All staff who are allocated a school laptop must use a secure, individual password to access software and documents held on the machine/server. Staff accounts can be accessed via any access point around school or via WIFI. The School Office and Head Teacher have access to their own PC's which are not on the main school network. Staff are allocated local administrator rights for their laptops in order to allow, for example, the installation of printers at home. Staff are encouraged to re-start their laptops in school in order to benefit from the full protection of Sophos Anti-Viral Software updates.

After use, or at the end of the day, Teachers and TA's must ensure that all users are logged out or have switched off.

Administrator rights for the school network are held by Mrs Worth (IT coordinator). She also has administrator rights for the school Outlook email accounts to manage staff emails, including resetting passwords and adding or deleting accounts. Mrs Worth also has Administrator Rights for Purple Mash.

All accounts for children or staff who leave Duke Street Primary School will be deleted immediately by Mrs Worth.

## Software/hardware:

All software or services purchased or used by the school have full user/site licences. Copies of these licences are available from Mrs Worth and they are renewed as required.

Mrs Worth carries out an annual audit of hardware and software in order to inform the Action Plan, and the School Secretary maintains a record of serial numbers of all ICT equipment for insurance purposes.

Staff will be able to download free apps to their teacher's iPad, using their own or a school Apple ID. Staff must seek authorisation before purchasing an app in order to be reimbursed.

## Managing the network and technical support:

The PC located in the school office has access to all admin records via SIMS. It is remotely backed up every day by the BT Lancashire Services. The curriculum server is located at various points across school. Technical support staff are able to access it for maintenance purposes. Right-Click ICT, Virtue Technology also have remote access.

All wireless devices are able to access the school network only by using a secure password. The security of the school network is managed by RightClick, BTLS and Virtue Technology. Safety issues will be regularly reviewed, or when a change is made to the network, e.g. as a server is replaced. Antiviral software (Sophos) is provided by the Virtue Technology, and updated weekly via the network.

Each member of the teaching/office staff and year group has a username and secure password to log onto the School network. Users may log on to the school network from any PC or laptop which is connected via cabling or WIFI, enabling access to software and documents located in their specific place on the server or in cloud storage. Pupils have restricted rights, e.g. they cannot access the control panel, or add/download software independently. This can only be carried out by the designated technician with full administrator rights.

Guests to Duke Street Primary School do not have username or passwords, but there are occasions when they would need to access programs on the server, for example a student or supply teacher. To access the network for teaching purposes they must first sign the relevant AUP before logging on.

All users are required to log out of the school system when finished, and to lock the screen before leaving the computer unattended. All computers and laptops should be switched off at the end of the school day in order to reduce Duke Street Primary School's carbon emissions, save money and allow automatic updates to be downloaded.
Pupils and Guests are not permitted to download programmes or install software, either to devices on the school network or iPads.

Staff are allowed to use school laptops for reasonable personal use at home, provided it is appropriate and does not contravene any of the conditions detailed in the AUP.

A member of staff who uses a school laptop must take personal responsibility for keeping a back-up copy of important resources e.g. planning, PowerPoints etc. used in lessons, in case of loss of or damage to that machine.

Should a member of staff wish to use a technical service for repair/maintenance issues other than that provided by the school, must first obtain permission from the Head teacher. Any charges incurred in this way will not be reimbursed by the school unless authorised in advance.

Should a member of staff be absent for a prolonged period of time, eg through sickness, sabbatical or maternity leave, their laptop and iPad device must remain in school until their return.

Any member of staff who uses a school laptop for personal use, eg to store music or their own images, to access bank or credit card details, use Social Network sites or Instant Messaging does so at their own risk, in the event of their personal details being obtained or used fraudulently, eg identity theft, hacking. Any applications or data stored on the laptop may be monitored. Duke Street Primary School accepts no responsibility for the loss of applications, data or files for personal use stored on a staff laptop in the event of loss by theft or irreparable damage. Staff are expected to take all reasonable care with their laptops when not on the school premises, e.g. they are not to be left in cars, loaned out or mistreated in any way.

Network monitoring takes place via Virtue Technology, and is in accordance with the General Data Protection Act (2018) Staff are aware of the monitoring and have signed the relevant AUP 's.

Staff have been made aware that the iPads are able to be tracked and monitored using Meraki Mobile Device Management.

Filtering and virus protection:

Duke Street Primary School has devolved control over the Sophos filtering service, managed by Virtue Technologies. We therefore operate 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 Teacher. 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. The Head Teacher may refuse to unblock a site.

Antiviral software (Sophos) is updated regularly to all staff laptops and school PC's via the network. In the event of a virus infection 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 Teacher, 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.

# 6 E-Safety across the curriculum

Duke Street Primary School aims to deliver effective Online Safeguarding education to all pupils through the delivery of the National Curriculum for Computing /EYFS. Regular, planned Online Safeguarding teaching is delivered within a range of curriculum areas including Computing, PSHE and Relationships Education. The Foundation Stage also provide age-appropriate Online Safeguarding learning opportunities. In addition, the School organises themed weeks focusing on Online Safeguarding awareness issues, around the annual Safer Internet Day event.

Learning is across several strands suggested including self-image and identity; online relationships; online reputation; online bullying; managing information online; health, wellbeing and lifestyle; privacy and security; copyright and ownership. Staff use the 'Education for A Connected World' document to inform teaching, planning and expected outcomes for each key stage.

At Duke Street Primary School, pupils in KS2 are also made aware of any specific issues or legislation contained in the General Data Protection Act (2018) or copyright implications in advance of any activity which may contravene this legislation e.g. the use of photographs or video clips. Pupils are made aware of the impact of online bullying during PSHE sessions and during School Assemblies. They are made aware of how to seek help if they are affected by these issues e.g. to contact a parent, trusted member of staff or even a friend. This includes radicalised or extremist online content. They are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

Class Teachers explain the significance of each point of the relevant AUP in order to ensure that pupils develop an understanding of the importance of the Acceptable Use Policy and adopt safe and responsible use of ICT both within and outside school. Posters of the AUP for pupils and reminders of safe Internet use are clearly displayed in each classroom.

## 6.1 E-Safety – Raising staff awareness

All members of staff have received Online Safeguarding training from the DSL at least once annually. The DSL, The Head teacher or ICT Advisor will provide advice/guidance or training to individuals as and when required or requested.

## 6.2 E-Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Duke Street Primary School offers regular opportunities for parents/carers and the wider community to be informed about Online Safeguarding, including the benefits and risks of using various technologies. This is done by social media and the school website.

## 6.3 E-Safety – Raising Governors' awareness

Governors are kept up to date with Online Safeguarding issues through briefings by the Head teacher and DSL at Governor meetings.

The Online Safeguarding Policy will be regularly reviewed and approved by the governing body.

## 7 Standards and inspection

We at Duke Street Primary school will monitor the effectiveness of the Online Safeguarding Policy by:

- Monitoring the Incident Log on CPOMS, to check for the frequency of incidents of inappropriate use, patterns in behaviour or of incidents
- Discussions with children to evaluate their level of awareness
- Ensuring AUP's are completed and filed, before access to ICT equipment or services at Duke Street Primary School
- Ensuring all Staff model and promote responsible use of ICT and digital resources.
- Ensuring all staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- Ensuring Online Safeguarding training provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safeguarding Policy and Acceptable Use Policy.
- Giving regular updates on Online Safeguarding Policy, Acceptable Use Policy, curriculum resources and ensuring general Online Safeguarding issues are routinely discussed in staff/team meetings.

Rachel Von-kaenel will feed back to the SLT/Governors and suggest appropriate actions/changes of policy or practice including the AUP's if needed.

Our ICT Co-ordinator will consult with RightClick ICT, Virtue Technology, ICT Advisors, and SMT the regarding Online Safeguarding implications of any future new technologies adopted in Duke Street Primary School.

Rachel Von-kaenel will ensure that all staff, pupils, parents/carers, visitors or other users of ICT equipment or services provided by Duke Street Primary School are kept fully informed of any changes, additions or issues regarding Online Safeguarding.

# APPENDIX 1

## 8. ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and governors are aware of their individual responsibilities when using technology. All staff members and governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in E-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of Mrs Worth.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's E-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

**User Signature**

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature...................................................... Date ........................................

Full Name .....................................................(PRINT) Position/Role ....................................................

# APPENDIX 2

## ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

**To be signed by any adult working in the school for a short period of time.**

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult.  I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

**User Signature**

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

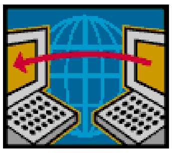
Signature ....................................................Date..............................................................................

Full Name .................................................(PRINT)Position/Role ..................................................

APPENDIX 3

## ICT Acceptable Use Policy (AUP) -Children FS/KS1

**These rules reflect the content of our school's E-Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren),understanding and agreeing to follow the school rules on using ICT, including use of the Internet.**

| **Think before you click** | |
|---|---|
| **S** | **I will only use the Internet when there is an adult in the room.** |
| **A** | **I will only click on icons and links that my teacher tells me or shows me.** |
| **F**  | **I will only send friendly and polite messages.** |
| **E** | **If I see something I don't like on a screen, I will always switch the monitor off and tell an adult.** |

**My Name: ___________________________________**

**My Signature: ________________________________**

**Parent / Carers Signature : _____________________**

APPENDIX 4

## ICT Acceptable Use Policy (AUP) -Children KS2

**These rules reflect the content of our school's E-Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.**

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into the classroom unless
- specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

**Signed** ........................................................................................................................ **(Child)**

We have discussed this Acceptable Use Policy and ............................................................ [Print child's name]
agrees to follow the E-Safety rules and to support the safe use of ICT at *Duke Street Primary School*
Parent /Carer Name (Print)....................................................................................................................

Parent /Carer (Signature) .......................................................................................................................

Class ................................................. Date ........................................................................................