Scotforth St Paul's
C of E Primary & Nursery School

Learning, growing and
caring as part of God's family

"I am the vine, and you are the branches.
If any remain in me and I remain in them,
they produce much fruit." (John 15:5)

Online safety policy

Last reviewed on:	September 2021
Next review due by:	September 2022

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying. It also includes disclosure of personal information, online reputation and well-being (considering amount of time spent online).
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will consider online safety within the curriculum committee, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of

recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead/deputies

Details of the school’s DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular updates on online safety in school to the headteacher and/or governing board

3.4 The Computing Subject Leader/Online Safety Champion

The Computing Subject Leader/Online Safety Champion is the main point of contact for Online Safety related issues and incidents. The role of the Online Safety Champion includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school’s Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP) ans SWGFL.
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school’s DSL to ensure a coordinated approach across relevant safeguarding areas

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3), and ensuring that pupils follow the school’s terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Infrastructure and technology

School ensures that the infrastructure/network is as safe and secure as possible. School subscribes to the Lancashire Grid for Learning Broadband Service and so internet content filtering is provided by default. It is important to note that the Netsweeper filtering service offers a high level of protection but very occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription and is installed on computers in school by LCC Education Digital Services then configured to receive regular updates.

4.1 Access

Children's access

- Children are always supervised when accessing school equipment and online materials (e.g. working with a trusted adult). Use of the computers at break and during lunchtimes is prohibited unless supervised by a member of staff.
- Children access the school systems using individual logins and age appropriate passwords.
- Children's access is restricted to certain areas of the network and computer.
- Children are taught how to stay safe online and must follow school's policies and practice
- Parents are asked to support school in ensuring their children follow school's AUP (Acceptable Use of the Internet Policy) and procedures.

Adult access

- Access rights to school systems are allocated to all staff according to their areas of responsibility

Passwords

- All adult users of the school network have a secure username and password. The administrator password for the school network is only available to HT and IT Technician.
- Staff and children are reminded of the importance of keeping passwords secure. Passwords can be changed at the individual's discretion by consultation with the HT/Computing Subject Leader.
- Passwords for children are made up by the children, with increasing complexity as they age. They are taught to keep them secret.

4.2 Software/hardware

- School has legal ownership of all software (including apps on tablet devices).
- School keeps an up to date record of appropriate licenses for all software. This is maintained by the Computing Subject Leader with the assistance of the ICT Technician and school Business Manager.
- An annual audit of equipment and software is made by the IT Technician/ Computing Subject Leader and Office Staff.
- The Computing Subject Leader, IT Technician and the head teacher control what software is installed on school systems

Managing the network and technical support

- Any servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have been security enabled.
- All wireless devices are accessible only through a secure password.
- Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases.
- LAA Education Digital Services are responsible for managing the security of our school network. This is monitored by LCC.
- School systems are kept up to date regularly in terms of security e.g. computers are regularly updated with critical software updates/patches and Sophos antivirus software is automatically updated.
- Users (staff, children, guests) have clearly defined access rights to the school network e.g. They have a username and password and, where appropriate, permissions are assigned
- Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended.
- Users are not allowed to download executable files or install software. The IT Technician possess administrator rights and is responsible for assessing and installing new software.
- Users can report any suspicion or evidence of a breach of security to the Computing Subject Leader, IT Technician or the head teacher.
- School equipment, such as teachers' laptops or cameras, should not be used for personal/family use
- Any network monitoring takes place in accordance with the Data Protection Act (1998) GDPR 2018. Staff are informed that the network may be monitored at any time and a regular (weekly) suspicious search query report is sent to HT.
- All staff, including The Computing Subject Leader and IT Technician have been provided with a copy of this policy and are aware of the standards required to maintain Online Safety in the school.

Filtering and virus protection

- IT system uses Netsweeper Filtering managed by LCC Education Digital Services.
- Prevent Duty - Light speed is complying with the Government's current Prevent Duty guidance. (See https://educationdigitalservices.lancashire.gov.uk/services/annual-services/broadband-bundle/internet-filtering.aspx for more details)
- Staff wishing to block or unblock websites may do so by making a request to the IT Technician who will liaise with HT if on doubt.
- The IT Technician ensures that all equipment, such as school laptops, used at home are regularly updated with the most recent version of virus protection used in school.
- Staff report any suspected or actual computer virus infection to the Computing Subject Leader or IT Technician

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 2,** pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Teaching of online safety is supplemented by input from the NSPCC, Coram Life Education and Police/PCSO on an annual basis.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be highlighted during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

9. Pupils using mobile devices in school

Children are not permitted to have mobile phones in school, except for Y5/6 who need them for safety when walking to/from school unaccompanied. The pupils must have the disclaimer signed by parents, and give their phones in to the teacher until the end of the day.

In the event of a non-authorised child bringing a mobile phone into school, the phone is removed and stored in the office. Parents are contacted to remind them of the school rules regarding mobile phones

This is in line with the acceptable use agreement (see Appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Staff using mobile devices in school

Staff are permitted to use personal mobile phones in school before the start of the school day, during break times, at lunch, after the school day has ended and during PPA. Mobiles must not be used where any pupils are present. The best place to use a mobile in school is the staffroom or office. Mobiles must not be linked to the school wifi.

Staff are responsible for the security of their own belongings, including mobile phones. They can store them securely in the school office on request. Staff are advised to store their mobile phones in 'silent' mode or off during lessons to reduce the risk of disturbance or inconvenience to others.

Images of children, video or audio must not be recorded on personal mobile phones.

The rules for mobile phone use in school apply to all other mobile devices. When permission to use such devices is granted it is expected that the relevant security settings, such as passwords and anti-virus protection, are in place and up to date.

The owners of the devices are responsible for ensuring that all the content held on them is legal and should understand that the school cannot be held liable e.g. for any damage or theft of personal devices.

Such devices can only be used by staff on the school's network, e.g. to transfer data by Bluetooth or to access the Internet using Wi-Fi, after obtaining the express permission of the head teacher and should be checked first to ensure that they contain no viruses or mal-ware that may cause damage to the school's systems. Staff are not allowed to connect to the school network for personal purposes, including using school wifi on mobiles.

11. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring anti-virus and anti-spyware software is updated as necessary by the IT technician
- Keeping operating systems up to date. Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.If staff have any concerns over the security of their device, they must seek advice from the IT technician.

12. Use of communication technology within school

Uy School uses a variety of communication technologies, each of which carries various benefits and associated risks. All new technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school.

Email

- The Lancashire Office 365 service is the preferred school email system
- Staff should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the head teacher and access is required for professional purposes.
- Children from Year 2 upwards have e-mail accounts within Purple Mash. Children and staff can communicate within this system, as necessary, which is secure and monitored.
- Only official school email addresses should be used to contact staff or parents.
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts
- All users should be aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail. Notices are displayed in staffroom of new SPAM outbreaks
- All users should be aware that email is covered by The Data Protection Act (1988), GDPR 2018 and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security
- All users should also be aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy
- Staff are responsible for monitoring the content of children's email communications, both outgoing and incoming messages.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Children are taught how to respond in such situations by reporting immediately to the adult in charge at that time. Staff report to senior leaders within the school and can report to Lancashire directly.
- Users should be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).
  Scotforth St Paul's school email disclaimer:
  ****
  CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.
- **
  All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social networks

See the Policy on the safe use of social networking sites and other forms of social media.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy and internet acceptable use policy for pupils. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

An incident log (see Appendix 4) is completed to record and monitor offences. This is audited on a regular basis by the head teacher. Any suspected illegal material or activity must be brought to the immediate attention of the head teacher who must refer this to external authorities, e.g. Police, CEOP Ceop.Police.uk/safety-centre/ or the Internet Watch Foundation (http://www.iwf.org.uk).

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headtecher and Computing Subject Leader. The review (such as the one available here from SWGFL) will inform changes in policy and practice.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Scotforth St Paul's
C of E Primary & Nursery School

Learning, growing and
caring as part of God's family

"I am the vine, and you are the branches.
If any remain in me and I remain in them,
they produce much fruit." (John 15:5)

Acceptable Use Policy

We live in an increasingly digital world where technology is part of our everyday lives. Digital technologies have the power to support and enhance teaching and learning. Our pupils are entitled to have safe access to, and use of, digital technologies in our school.

This Acceptable Use Policy is intended to ensure:

- That pupils stay safe and are responsible users of digital technologies for educational purposes
- That school systems and our users are protected from misuse
- That users are aware of the importance of staying safe online and being responsible digital citizens

All users of technology within our school must agree to certain rules and only use technology and software as instructed.

A copy of the E-Safety Policy is available on the school website, so that parents /carers are aware of the school's expectations of our staff and pupils.

The attached form is for the children to sign once it has been read and understood. Class teachers will go through the form to ensure the children understand their responsibilities.

My Responsibilities

I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, computers or the internet.

I will follow the stop, close and report procedure, should I see something that is inappropriate or that makes me feel uncomfortable on the internet.

I will report any suspected misuse or problems to a teacher.

I will make sure there is permission to use any material that I find.

I will make sure that I maintain a healthy lifestyle and won't spend too much time using technology.

I will treat all devices with care and respect, and understand that if a device is damaged, I must report it to the teacher as soon as it happens.

Cyberbullying

I understand that the school will not accept bullying in any form.

I will be careful with all communications making sure that anything I write cannot be mistaken as bullying.

I understand that I should report any incidents of bullying.

Access to Internet Sites

I will not try to access sites that are blocked or that are unsuitable for use in school. This includes social media websites, chat rooms and age restricted websites.

Communication – email, social networks, blog etc.

I will be careful in my communications making sure that nothing I write is offensive.

I will not write anything that could be seen as insulting to the school.

I will not share any personal information about myself or others on the internet or with sources I am not familiar with. (Personal information includes, name, address, age, gender, school name, e-mail address or phone number.)

Mobile Phones (Y5 and Y6)

If I need a mobile phone in school because I am walking home alone, my parents will send a letter to my teacher and I will give my phone to my teacher to look after during the school day.

Sanctions

I understand that the school will monitor my use of computers and other technology.

I understand that the school may investigate incidents that happen outside school.

I understand that there are regulations in place when pupils use ICT and that there are sanctions if I do not follow the rules.

Name ____

Signed ____

Class ____________________ Date ____________________

Appendix 2: acceptable use agreement (staff and volunteers)

Scotforth St Paul's
C of E Primary & Nursery School

Learning, growing and
caring as part of God's family

"I am the vine, and you are the branches.
If any remain in me and I remain in them,
they produce much fruit." (John 15:5)

Policy for Acceptable Use of Digital Technologies- Staff and Volunteers

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy.

This acceptable use policy is intended to ensure:

- That staff and volunteers are responsible users of digital technologies for educational and professional purposes
- That school systems, digital resources and users are protected from misuse
- That staff and volunteers are protected from potential risk in using digital technology in school

All users of technology within our school must agree to certain rules and only use digital technology, resources and software as instructed.

Acceptable Use Policy Agreement

I understand that I must use digital systems and resources responsibly, to help ensure my own safety and the safety and security of other users and the school systems.

For my professional and personal safety:

- I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
- I understand that the school's digital technology resources and systems are primarily intended for educational use and that I will only use them for Professional purposes or for uses specified within policies and rules set by the school.
- I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the appropriate person(s) if I suspect a breach.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

I will be professional in my communications and actions when using digital systems and resources:

- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will communicate with others in a professional manner.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will not use my personal equipment to record these images, unless I have permission to do so
- I will only use social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or breach confidentiality

When accessing digital systems and resources:

- I will not connect a device to the network / Internet that does not have up-to-date anti-virus software
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try to use any tools or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- I will not install or attempt to install software of any type on a machine nor attempt to change computer settings, unless this is permitted by the school
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority

When using the internet in my professional capacity:

- I will obtain the relevant permissions to use the work of others
- I will not download or distribute materials protected by copyright (including music and videos)

I understand that I am responsible for my actions inside and outside of school:

- I understand that this acceptable use policy applies not only to my work and use of school technology equipment at school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I understand that it is my responsibility to ensure I remain up to date and understand the school's most recent online safety and safeguarding policies.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ____

Signed: ___________________________________

Date: __________________________

Appendix 3: acceptable use agreement (students/supply)

The following statements outline what we consider to be acceptable and unacceptable use of Mobile phones:

- Staff/visitors are permitted to use personal mobile phones in school before the start of the school day, during break times, at lunch, after the school day has ended and during PPA. Mobiles must not be used where any pupils are present. The best place to use a mobile in school is the staffroom or office. Mobiles must not be linked to the school wifi.
- Staff/visitors are responsible for the security of their own belongings, including mobile phones. They can store them securely in the school office on request.
- Staff/visitors are advised to store their mobile phones in 'silent' mode or off during lessons to reduce the risk of disturbance or inconvenience to others. Images of children, video or audio must not be recorded on personal mobile phones.
- Children are not permitted to have mobile phones in school, except for Y5/6 who need them for safety when walking to/from school unaccompanied. The pupils must have the disclaimer signed by parents, and give their phones in to the teacher until the end of the day.
- If mobile phones are brought into school by a pupil who does not have authorization, they will be kept in the School Office until the end of the school day and then passed to parent/carer

For use by any adult working in the school for a short period of time:

1. I have read and understand the school's policy on the use of mobile phones and similar devices

2. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally

3. As a visiting supply/student teacher I will be assigned a network log-in, allowing me limited access to the school network, sufficient to carry out my duties.

4. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory

5. I will respect copyright and intellectual property rights

6. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy, on school equipment and with written consent of the parent/carer or relevant adult

7. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image

8. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems

9. I will not install any hardware or software onto any school system or use school wifi on personal devices

10. 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

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

Signature …………………………………………………………………………………… Date ………………………………………

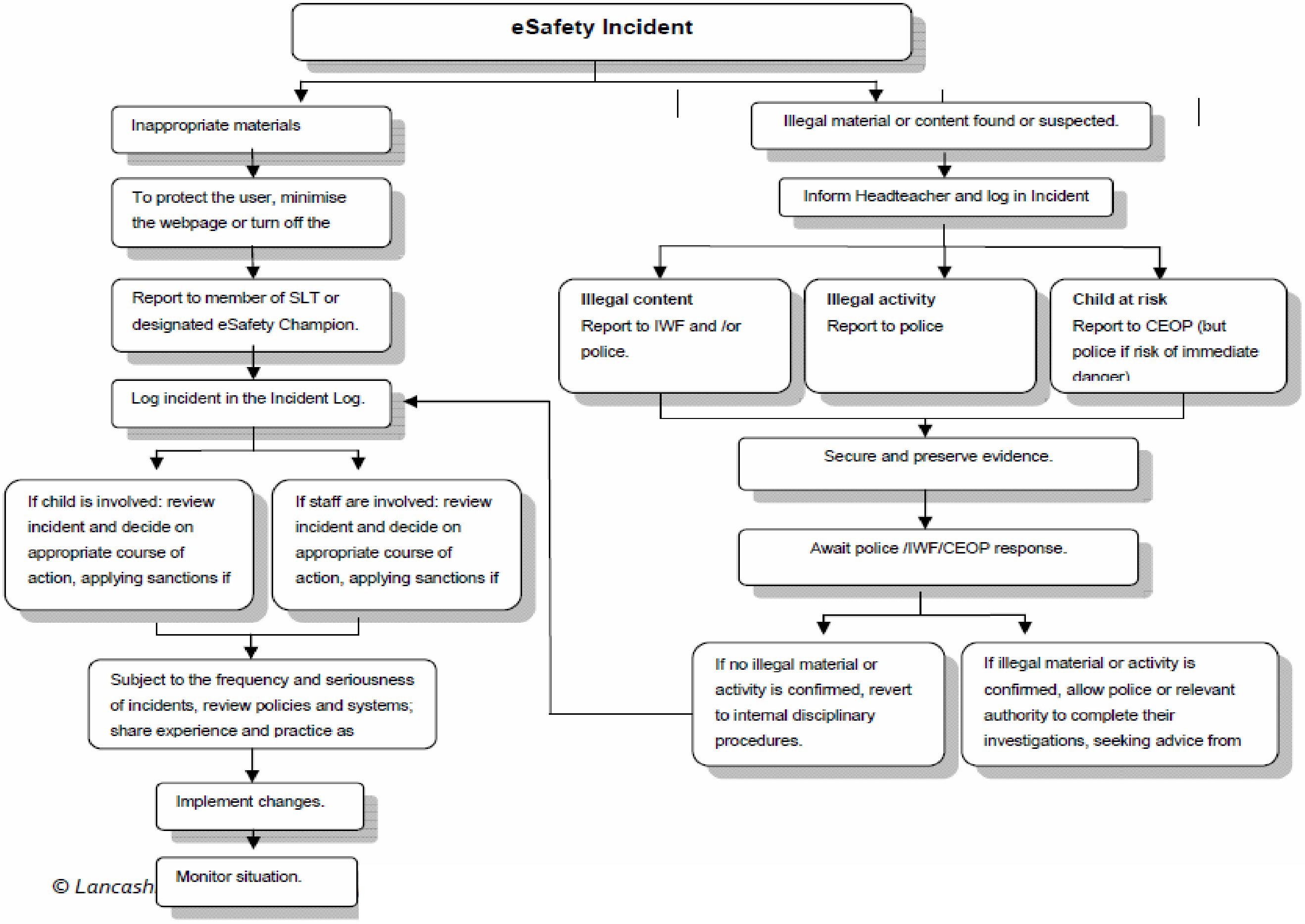
Full Name & Position / Role …………………………………………………………………………………………………… (PRINT)

Appendix 4: online safety incident log

All Online Safety incidents must be recorded by the School Online Safety Champion, or designated person. This incident log will be monitored, and reviewed regularly by the Head teacher and Chair of Governors. Any incidents involving cyberbullying should also be recorded on the Integrated Bullying and Racist Incident Record Form 2 available via the Lancashire Schools Portal. Completed forms will be scanned and uploaded to CPOMS. If necessary it will also be entered into the Serious Incident Book.

Date / Time of Incident	**Type of Incident**	**Name of pupil/s and staff involved**	**System details**	**Incident details**	**Resulting actions taken and by whom (signed)**
01 Jan 2015 9.50 am	Accessing inappropriate website	A N Other (Pupil) A N Staff (Class Teacher)	Class 1 Computer	Pupil observed by Class Teacher deliberately attempting to access adult websites	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.

Appendix 5: responding to an online safety incident



eSafety Incident

Inappropriate materials

To protect the user, minimise the webpage or turn off the

Report to member of SLT or designated eSafety Champion.

Log incident in the Incident Log.

If child is involved: review incident and decide on appropriate course of action, applying sanctions if

If staff are involved: review incident and decide on appropriate course of action, applying sanctions if

Subject to the frequency and seriousness of incidents, review policies and systems; share experience and practice as

Implement changes.

Monitor situation.

Illegal material or content found or suspected.

Inform Headteacher and log in Incident

Illegal content
Report to IWF and /or police.

Illegal activity
Report to police

Child at risk
Report to CEOP (but police if risk of immediate danger)

Secure and preserve evidence.

Await police /IWF/CEOP response.

If no illegal material or activity is confirmed, revert to internal disciplinary procedures.

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from

© Lancash

Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp

LCC Schools' eSafety Lead

Lancashire Schools' ICT Centre

graham.lowe@ict.lancsngfl.ac.uk

Securing and Preserving Evidence – Guidance Notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system).
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
- Make a note of the date / time of the incident along with relevant summary details.
- Contact your School's Neighbourhood Policing Team for further advice.