Little Plumstead Church of England VA Primary School

Policy for Online Safety 2018

Introduction

As a Church school we want to help our pupils be citizens of the world. We believe that knowledge and understanding of the online world is essential to help achieve this aim. We believe it is also essential to be able to access this world safely and confidently and with due respect for all. It is with this in mind that we regularly develop our online safety policy.

1. Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for computing, bullying and for child protection.

The school will identify a member of staff who has an overview of Online Safety, this would usually be the Senior Designated Professional (SDP).

Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

The Online Safety Policy and its implementation will be reviewed annually.

The Online Safety Policy was discussed by Staff

The Online Safety Policy was revised by the Deputy Head.

It was approved by the Governors in October 2018

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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. It also takes into account the Data Protection Act 2018.

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

3. Overview

3.1 Roles and Responsibilities

The Governing body are responsible for the approval of this policy and reviewing its effectiveness. This should be achieved through an Online Safety continuous item on Teaching and Learning Committee meetings where current effectiveness is monitored and fed back to the full governing body.
The Headteacher has a duty of care for ensuring the safety of all members of the school community. Much of this responsibility can be delegated to the Online Safety Leader.

Responsibilities of the Online Safety Leader can be found in their terms of reference.

The network manager (ICT technician) will ensure the school's technical infrastructure is not open to misuse and is fit for purpose.

The school Internet access is provided by Updata and includes filtering appropriate to the age of pupils.

Teachers have a responsibility to:

- Adhere to the Staff/Volunteer Code of Conduct
- Report any concerns to the Online Safety Coordinator
- Embed the Online Safety curriculum throughout all classroom learning (SWGfL CommonSense Education Digital Literacy and Citizenship)

Pupils will:

- Adhere to the Responsible Use Agreement
- Uphold good Online Safety practice when out of school

Parents will sign their child's Responsible Use Agreement and promote safe use of technology outside of school.

3.2 Curriculum

The curriculum will be reviewed with respect to Online Safety, by the Teaching and Learning committee.
Current Practice:
As part of our curriculum, we teach regular digital literacy and citizenship lessons. The programme of study can be found on the school website. Teachers choose activities from each lesson heading to cover each half term. We also refer to this learning whenever we use online resources in other subjects. The digital literacy and citizenship lessons cover internet safety, privacy and security, relationships and communication, cyberbullying, digital footprint and reputation, self-image and identity, information literacy and creative credit and copyright. The lessons are age-appropriate and coverage is spread across the school. Reception children discuss online safety in their class at an appropriate level, led by the teacher when relevant.

Pupils will be taught Online Safety, across all subjects, and have messages reinforced in assemblies and wider school activities (e.g. Safer Internet Day).

Pupils will be taught acceptable and effective use of the Internet.

Pupils will be shown how to publish and present information appropriately to a wider audience. The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content and behaviour in line with this policy.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list (if possible) for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.3 Training and Induction

Teaching Staff

A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly by the Teaching and Learning committee. All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and School/Volunteer Code of Conduct.

Parents/Carers

It is important that parents/carers are also informed and, where needed, educated on Online Safety matters. This should be done through regular updates through a variety of communication streams, such as: newsletters, the school website, Online Safety meetings and parents' evenings.

Governors

Governors involved in this area should receive suitable training.

4. Managing Internet Access

4.1 Information system security

School ICT systems security will be reviewed regularly by the Teaching and Learning committee. Virus protection will be updated regularly.

Security strategies will be discussed with the Local Authority.

4.2 E-mail

Pupils and staff may only use designated email accounts on the school system:

- Norfolk Schools Internet Exchange (NSIX)
- Accounts from the .norfolk.sch.uk domain (e.g office@littleplumstead.norfolk.gov.uk)

Pupils must immediately tell a member of staff if they receive an offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school will consider how e-mail from pupils to external bodies is presented and controlled.

4.3 Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.

The headteacher has overall editorial responsibility and will ensure that content is accurate and appropriate.

4.4 Publishing photographs, images and work

Photographs that include pupils will be selected carefully and will not include identifiable images of pupils whose parents/carers have requested their child's/children's images are not to be used outside school.

Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs or images of pupils are published see Pupil Esafety Responsible Use and Parental Consent for Use of Photographs, Digital Images and Videos)

Written permission from adults will be obtained before their names, photographs or images of themselves are published (see Staff/Volunteer Code of Conduct).

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories (see Parental Consent for Use of Photographs, Digital Images and Videos).

4.5 Social networking and personal publishing on the school learning platform

The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords, sharing images etc.

All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

Pupils, parents and staff will be advised on the safe use of social network spaces.

Pupils will be advised to use nicknames and avatars when using social networking sites.

4.5 Managing filtering

The Online Safety leader will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to any member of staff who must follow reporting procedures (see Section 4.4).

The Online Safety leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.6 Managing Videoconferencing

Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

4.7 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.8 Other devices

Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity (see section 3.9).

The sending of abusive, offensive or inappropriate material is forbidden.

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering and care will be taken with their use if it is necessary within the school use. The school has a Nintendo Wii which comes into this category

Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

4.9 Bring Your Own Device (BYOD)

It is understood that there are many opportunities when staff and pupils may want to use their own devices on the school system. Usually for pupils this would only be to contact parents and their device will be handed in to the school office at the beginning of the day and collected at the end.

Staff, visitors and pupils will adhere to their respective Responsible Use Agreements.

Pupils use these devices at their own risk and the school cannot be held responsible for loss or damage.

4.10 Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

5. Policy Decisions

5.1 Authorising Internet access
All adults (either staff or member of the community) must read and sign the Staff/Volunteer Code of Conduct before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Parents will be asked to sign and return the Responsible Use Agreement.

Pupils must agree to comply with the Responsible Use Agreement statement before being granted Internet access.

5.2 Community use of the Internet
All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy.

5.3 Assessing risks
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

5.4 Handling Online Safety Incidents
Incidents should be dealt with according to the flow chart (**Appendix A)**

All Online Safety incidents or Internet misuse will be dealt with by the Online Safety Coordinator and a senior member of staff.

Any complaint about staff misuse must be referred to the Online Safety Coordinator and Headteacher.

Complaints of a child protection nature must be referred to the Online Safety Coordinator and Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.

If there is a complaint regarding the Online Safety Coordinator then another senior member of staff or Chair of Governors should be informed.

Pupils and parents will be informed of the complaints procedure.

Pupils and parents will be informed of consequences for pupils misusing the Internet.

6. Communications Policy

6.1 Introducing the Online Safety policy to pupils
Appropriate elements of the Online Safety policy will be shared with pupils.

Online Safety rules will be posted in all networked rooms.

Pupils will be informed that network and Internet use will be monitored.

Curriculum opportunities to gain awareness of Online Safety issues and how best to deal with them will be provided for pupils.

6.2 Staff and the Online Safety policy

All staff will be given the school Online Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues**.**

6.3 Enlisting parents' support

Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school web site.

Parents and carers will, from time to time, be provided with additional information on Online Safety.

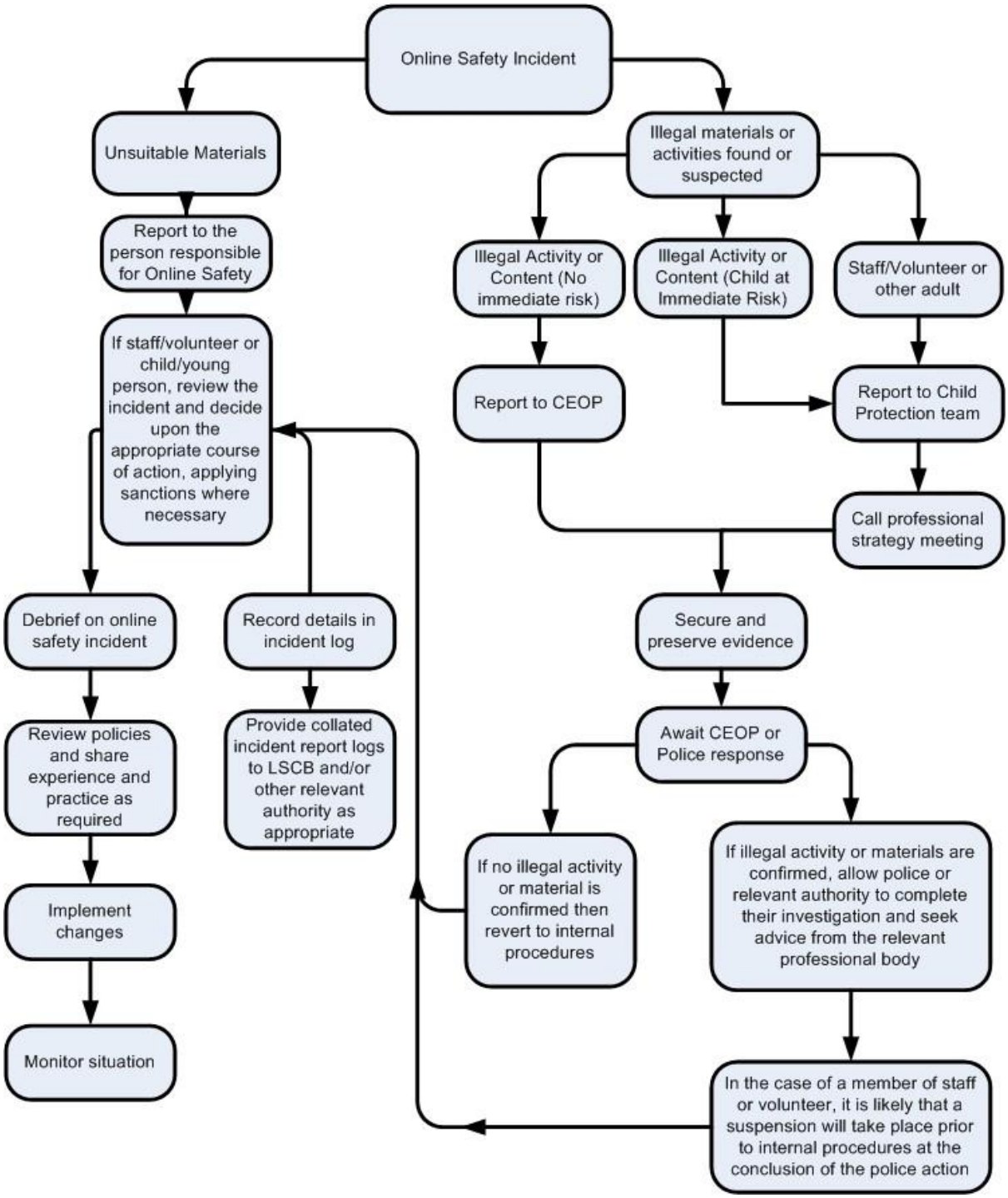
The school will ask all new parents to sign the Responsible Use Agreement when they register their child with the school.

Drawn up by: Deputy Head

Date approved by governors: November 2018

Next review date: Autumn 2019

Appendix A - Incident Reporting Flow Chart



Appendix B - Online Safety Leader Terms of Reference

Online Safety Leader Terms of Reference

1. Overview

The Online Safety leader develops and maintains an eSafe culture within the school and oversees all digital safeguarding within the school.

2. Responsibilities

The key responsibilities of the Online Safety leader are:

- developing an eSafe culture.
- being the main point of contact on issues relating to e-safety
- raising awareness and understanding of Online Safety issues amongst all stakeholders, including parents and carers.
- embedding Online Safety in staff training, continuing professional development and across the curriculum and learning activities.
- keeping a log and reporting on Online Safety incidents.
- keeping up with relevant Online Safety legislation.
- liaising with the local authority and other agencies as appropriate.
- reviewing and updating Online Safety policies and procedures regularly.

3. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

Signed by (SLT): .....

Date:.....

Date for review (annually):.....

Apppendix C - Responsible Use Agreement

ONLINE SAFETY

Responsible Use Agreement

Name of Child:..... **Class:**.....

We use the school devices and the Internet for learning. These rules will help us to be fair and keep everyone safe:-

- I will ask permission before entering any websites or app, unless my teacher has previously approved its use.
- On a network, I will only use my own login and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will only e-mail people I know and my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail or on the Internet I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat (with the exception of school approved e communities)
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or other devices.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of websites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer systems is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

I have read and understood the school rules for Responsible Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

I understand that if I break these rules then I may not be allowed to use school devices.

Pupil's signature ..... Date.....

(or parent's signature on behalf of the pupil following the parent reading and explaining the above agreement to their child, if the pupil is unable to read and understand the above Responsible Use Agreement)

PTO FOR PARENT/GUARDIAN'S ACKNOWLEDGEMENT

Parent's/Guardian's Acknowledgement

I have read and understood the school rules for responsible Internet use.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that the school is not liable for any damages arising from the use of Internet facilities.

Parent's/Carer's signature ..... Date .....

School

The school acknowledges the above signatures and therefore grants Internet access.

Signed: ..... Date: ……

(Online Safety Leader)

FOR OFFICIAL USE ONLY
For a child in breach of the agreement, the log below will be kept by the school.

Date	**Notes**	**Action**

Appendix D - Staff/Volunteer Code of Conduct

Introduction:

Computing, ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will encourage Online Safety with pupils in my care and model best practice at all times.
- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet / Social media accounts and any related technologies for uses permitted by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username
- I will ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.

- At school, I will not install any hardware or software without the permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory or could knowingly put the school's network at risk.
- I will not engage in online activity that may compromise my professional responsibilities in and out of school.
- Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Headteacher.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head teacher.

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

Permission for Photograph and Film
I agree/disagree* to photographs and films featuring my image being stored and used responsibly on the school website and social media platforms.
* delete as appropriate

Full name:……..…(printed)

Job title:……..…

Signature:……Date:……

Appendix E - IRIS Policy

1. Overview

IRIS is a 'self-videoing' system of staff development. Teachers and other staff can record their teaching and then reflect back on their practice either alone, or, ideally, as part of a pair or group.

2. Filming with IRIS

Staff should notify a member of staff (usually the Online Safety leader) when they are using the equipment

Children must be informed when they are being filmed.

IRIS must not be used during any period where children are changing; for example PE lessons.

3. Viewing Reflections

Staff are permitted to view reflections at home and should maintain the standards described in the Staff/Volunteer Code of Conduct.

If staff are concerned about anything they have viewed in the reflection they should contact the Online Safety Coordinator or follow school safeguarding procedures.

4. Editing

The editing features should be used to highlight a specific area of practice.

It recommended that staff edit their own videos; however, if editing for another member of staff, do so in accordance with the Staff/Volunteer Code of Conduct Policy agreed by staff on:.....

Appendix F – Online Online Safety Audit

Online Safety Checklist

This checklist can be used to carry out a very simple audit of the online safety provision in your school. A more thorough audit is carried out annually, using the 360 Degree self-review online tool.
360 Degree self-review link:
http://swgfl.org.uk/products-services/Online Safety/services/360

Basic Audit:

The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
Has the school got an online safety Policy that allies with Norfolk guidance?	**Y/N**
When was the policy updated/reviewed?	
The school online safety policy was agreed by governors on:	
How is the policy made available for staff? :	
How is the policy made available for parents/carers?:	
Is a clear, progressive online safety education programme in place for all pupils?	**Y/N**
Are all pupils aware of the School's ICT Code of Conduct/Acceptable Use Policy?	**Y/N**
Are online safety rules displayed in all rooms where technologies are used and expressed in a form that is accessible to all pupils?	**Y/N**
Has up to date online safety training been provided within the last year for staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Do all staff receive and sign an ICT Code of Conduct on appointment?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School ICT Code of Conduct/Acceptable Use Policy?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Is Internet access provided by an Internet service provider which complies with DfE/NEN requirements?	**Y/N**
Have online safety materials from CEOP been obtained?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act, following guidance provided by the ICO?	**Y/N**
Where appropriate, have teaching and/or technical members of staff attended training on the school's filtering system?	**Y/N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Y/N**

Appendix G – Reporting

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct/AUP and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

Appendix H – Parental consent for use of photographs, digital images and videos

PARENTAL CONSENT FOR USE OF PHOTOGRAPHS, DIGITAL IMAGES AND VIDEOS

PUPIL'S NAME	

At Little Plumstead CE VA Primary School, we sometimes take photographs of pupils. We use these photos in the school's parent handbook and publications, on the school's website and twitter account and on display boards and display screens around school.

We really value using photos of pupils to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

This consent form will be valid until your child leaves the school. However if you change your mind at any time, you can request a new consent form for completing by emailing office@littleplumstead.norfolk.sch.uk, calling the school on 01603 712165, or just popping in to the school office.

Please tick the relevant boxes below and return this form to school.

GROUP PHOTOGRAPHS, DIGITAL IMAGES AND VIDEOS

I consent for photographs, digital images and videos to be taken of my child in GROUPS of 2 or more pupils for the following purposes:

	✓
In internal displays and classroom resources	
The school website	
The school's twitter account	
The school's newsletter	
The school's parent handbook and publications	
School powerpoint presentations	
My child's image in group situations to be included in the work books of other children	
Official annual class photograph taken by an external photographer authorised by the school to do	
The school to share photos with the local media in connection with a school event or activity	
The school to retain photos and videos for historical purposes when my child leaves the school	

PLEASE TURN OVER FOR CONSENT FOR INDIVIDUAL PHOTOS, DIGIAL IMAGES AND VIDEOS

INDIVIDUAL PUPIL PHOTOGRAPHS, DIGITAL IMAGES AND VIDEOS

I give consent for individual photographs, digital images and videos to be taken of my child for the following purposes:

	✓
In internal displays and classroom resources	☐
The school website	☐
The school's twitter account	☐
The school's newsletter	☐
The school's parent handbook and publications	☐
School powerpoint presentations	☐
Official annual school photograph taken by an external photographer authorised by the school to do	☐
The school to share photos with the local media in connection with a school event or activity	☐
The school to retain photos and videos for historical purposes when my child leaves the school	☐

Parent's/Carer's signature: ……

Date: ……