Woodford Church of England Primary School

Online Safety Policy

October 2019

Contents

Please refer to Keeping Children Safe (2019) and Teaching online safety in school (2019) for more guidance or refer to Education for a Connected World Framework for age specific advice.

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Woodford Church of England Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Woodford Church of England Primary School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online (Internet or gaming)).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Our Computing curriculum and whole school approach will therefore concentrate on the five main areas:

- How to evaluate what you see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

This policy applies to all members of our school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices

and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
Our school will deal with such incidents within this policy and where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Role	Key Responsibilities
Principal / Academy Trust	• To take overall responsibility for Online Safety provision. • To take overall responsibility for data and data security (GDPR.) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious Online Safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator and technician.

Online Safety Lead (Computing Lead)	• Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents.
	• Promotes an awareness and commitment to e-safeguarding throughout the school community.
	• ensures that Online Safety education is embedded across the curriculum
	• Liaises with school ICT technical staff.
	• To communicate regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
	• To ensure that an Online Safety incident log is kept up to date via MyConcern.
	• Facilitates training and advice for all staff.
	• Liaises with the Local Authority and relevant agencies.
	• Is regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • Sharing of personal data.
	  • Access to illegal / inappropriate materials.
	  • Inappropriate on-line contact with adults / strangers.
	  • Potential or actual incidents of grooming.
	  • Cyber-bullying and use of social media.
	• To oversee the delivery of the Online Safety element of the Computing curriculum.

Governors / Online Safety governor	• To ensure that the school follows all current Online Safety advice to keep the children and staff safe. • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out upon receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. • To support the school in encouraging parents and the wider community to become engaged in Online Safety activities. • The role of the Online Safety Governor will include: Regular review with the Online Safety Co-ordinator including Online Safety incident logs, filtering / change control logs.
Network Manager / technician At Woodford C of E Primary School	• To report any Online Safety related issues that arises, to the Online Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.

	• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date.
	• To ensure the security of the school ICT system.
	• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.
	  • The school's policy on web filtering is applied and updated on a regular basis.
	  • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
	• To keep up-to-date documentation of the school's e-security and technical procedures.

Bursar	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
Teachers	• **To embed Online Safety issues in all aspects of the curriculum and other school activities.** • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant.) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's Online Safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Agreement. • To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the Online Safety coordinator. • To maintain an awareness of current Online Safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use agreement (NB: KS1: sign a simplified version and Reception agree safety rules together as a class.) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation/ review of Online Safety policies.

Parents/Carers	• To support the school in promoting Online Safety and endorse the Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children. • To consult with the school if they have any concerns or issues.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints:

- The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring

- The school has an Online Safety coordinator who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors.

2. Education and Curriculum

Pupil Online Safety curriculum
This school

- Has a progressive Online Safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To zip it, block it and report it.
    - To follow the SMART rules displayed in each classroom.
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
    - To know how to narrow down or refine a search.
    - [For older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.

- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- [For older pupils] to understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Has a whole school approach to embedding online safety through all lessons. Every time technology is used within a lesson there is an opportunity to discuss an online safety concept. The discussion and references to staying safe are an embedded part of every day teaching.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Agreement which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on Online Safety issues.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Agreement.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site; placed on windows around the school site.
  - Demonstrations, practical sessions held at school.
  - Suggestions for safe Internet use at home.
  - Provision of information about national support sites for parents.
  - Providing training.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- Are responsible for reading the school's Online Safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online Safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school:

- There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) 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. The records are reviewed, audited and reported to the school's senior leaders.
- Parents / carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use.
- Never allows/ Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the Headteacher.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access.
- We provide pupils with an individual network log-in username.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.

- Uses our broadband network for our CCTV system and have had set-up by approved partners.
- All computer equipment is installed professionally and meets health and safety standards.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This school

- Provides staff with an email account for their professional use.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Has the option to give pupils their own email address to be used within school (age dependent).

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- Uploading of information is restricted to teachers and admin staff.

Social networking

Social networking applications include, but are not limited to:

- Blogs, for example Blogger, Twitter.
- Online discussion forums, such as netmums.com.
- Collaborative spaces, such as Facebook.
- Media sharing services, for example YouTube.

Use of Social networking sites in worktime

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Head teacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first.

- The school will block/filter access to social networking sites as much as possible.
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space.
- They should consider how public the information is and consider using private areas.
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The profession is not brought into disrepute.
- They are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.

In the event of staff misuse

If an employee is believed to have misused the internet or setting network in an illegal, inappropriate or abusive manner, a report must be made to the Principal immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- Local Authority Safeguarding and Quality Assurance Service Office – 01604 654040.
- Police/CEOP (if appropriate).

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed only if appropriate.

Social media and the prevent duty

Staff are made aware of the ways social media methods are used to encourage extremist behaviour in young people. This can include:

- Facebook.
- Twitter.
- Youtube.
- AskFM.
- Tumblr.
- Personal messaging including WhatsApp, Kik, SureSpot and Viber.

Children are taught which websites are safer for children to use i.e. KidRex.

Any staff with concerns regarding children access to extremist material should report these to the Designated Safeguarding Lead as soon as possible.

Video Conferencing

This school

- Only uses approved or checked webcam sites.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- All staff are DBS checked and records are held in one central record.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement . We have a system so we know who has signed.

- staff
- governors
- pupils

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the school office arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Staff use of personal devices

- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their Online Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.