Walter Infant School and Nursery

ONLINE SAFETY POLICY

Document History

Version	Action	By	Date
1	Approved	Full Governing Body	17th February 2022

'To be the best I can be'

Responsibility of: The Full Governing Body

Date of Review: Spring Term 2024

1. Aims

Walter Infant School and Nursery 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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 Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL)

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 3)

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 and Deputy Designated Safeguarding Lead

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Computing Lead and other staff, as necessary, to address any online safety issues or incidents;
- 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 a termly update on online safety for the Governing Body.

This list is not intended to be exhaustive.

3.4 The Senior Leadership and Administration Team

Our Senior Leadership Team and Administration Team along with our Computing Support Team, Watermans Solutions are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

This list is not intended to be exhaustive.

3.5 The Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk. SLT should be informed where school policies may require updating.

3.6 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;

This list is not intended to be exhaustive.

3.7 Parents and Carers

Parents and Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- Ensure their child has understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2);

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

- Childnet International Hot topics
- Childnet International Parent factsheet
- Disrespect Nobody Healthy relationships
- Commonsensemedia Provides independent reviews, age ratings and other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- National Crime Agency/CEOP Thinkyouknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

3.8 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. Educating pupils about online safety

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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

To meet our aims and address the risks above we will:

- Educate pupils about online safety as part of our curriculum using our bespoke online safety programme Robot: For example:
    - The safe, respectful and responsible use of social media, the internet and technology;
    - Keeping personal information private;
    - How to recognise acceptable and unacceptable behaviour online;

- Identify a range of ways to report concerns about content and contact;
- How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they are a witness rather than a victim.

By the end of Year 2, they 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 be aware that any 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;
- 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.

Walter Infant School and Nursery will:

- Train staff, 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.
- Educate parents/carers about online safety via our website, communications sent directly to them, safeguarding items in the Newsletter and during Parents' Information Evenings. We will also share with them the procedures so they know how to raise concerns about online safety;
- Ensure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
  - Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present;
  - Staff will not take pictures or recordings of pupils on their personal phones or cameras.
- Make all pupils (and their parents and carers), staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology;
- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation

- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's ICT systems
- Carry out an annual review of our approach to online safety;

5. Educating parents and carers about online safety

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

Online safety will also be covered during an annual parents' and carers' information evening either in school or virtually.

If parents or carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

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

6. Cyber-bullying

6.1 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's Behaviour Policy and Staff Code of Conduct.)

6.2 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. All teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Relationships and Health Education (PSRHE) and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school will also share information on cyber-bullying to parents and carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

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.

6.3 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 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.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All pupils, parents, carers, staff, volunteers and governors 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, governors 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.

7.1 Storage and deletion

- All images of pupils will be securely stored in one central location.

- Where memory cards, USB drives or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
- Images of pupils should normally be deleted once a pupil has left the school unless being kept as part of archived records. Such retention, and the period involved, should be specified in the Data Protection or Data Retention policy.

8. Using mobile devices in school

Pupils will not bring phones to school. Any phones brought in by mistake will be collected at the start of the day and stored securely until home time. Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.

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.

- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- Schools should be vigilant where mobile phones are used with children in the Foundation Stage. Staff, helper and visitor mobile devices may normally be switched off or on silent during the times that children are present.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9. Staff using work devices in and out 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;

- Keeping operating systems up to date – always install the latest updates;

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 3.

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 our computer support team.

9.1Communication with Parents and Children

- Teachers must only use their school email address when communicating with parents via email;
- Teacher/parent contact should normally be by the main school telephone and not via a personal mobile device. An exception would be where a teacher may be working from home and is making a prearranged call under the direction of the Leadership Team. In this case, the mobile number must be withheld;
- All lessons required to be available online, will be pre-recorded;
- In the event of a prolonged school closure, class Zoom meetings may be arranged for the purpose of keeping in touch. Only invited guests will be allowed to join through a waiting room. A risk assessment for the meetings will be produced and shared with all participants before the meetings take place.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will contact parents or carers immediately. 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 Disciplinary Policy and Procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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).

The DSL and Deputy DSL 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 be invited to attend 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.

12. 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 annually by the Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This policy is linked to the following policies:

- Child Protection and Safeguarding
- Staff Code of Conduct
- Behaviour
- Staff disciplinary
- Privacy notices
- Complaints

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only;
- Only use them when a teacher is present, or with a teacher's permission;
- Keep my username and passwords safe and not share these with others;
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- Tell a teacher (or other adult) immediately if I find any material which might upset, distress or harm me or others;
- Always log off or shut down a computer when I'm finished working on it.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher;
- Use any inappropriate language when communicating online, including in emails;
- Log in to the school's network using someone else's details;
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

Pupils will not bring a personal mobile phone or other personal electronic device into school.

Parents and Carers will not use a mobile device on the school site unless permission is given by a member of the senior leadership team, for example to phone another parent or carer about a collection arrangement (password).

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and that no personal electronic devices will be brought into school, and will make sure my child understands the reasons for these restrictions.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material); • Use them in any way which could harm the school's reputation; • Access social networking sites or chat rooms; • Use any improper language when communicating online, including in emails or other messaging services; • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network; • Share my password with others or log in to the school's network using someone else's details; • Take photographs of pupils without checking with teachers first; • Share confidential information about the school, its pupils or staff, or other members of the community; • Access, modify or share data I'm not authorised to access, modify or share; • Promote private businesses, unless that business is directly related to the school.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**