Water Hall Primary School
Online Safety Policy

Person responsible:	Adele Howson	
Approved by:	Water Hall Academy Improvement Board	
Last reviewed on:	November 2021	
Next review due by:	November 2022	

Contents

---

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
- 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 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.
The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Academy Improvement Board (AIB)

The AIB has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will coordinate regular meetings with appropriate staff to discuss online safety, 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

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

Details of the school's DSL and other safeguarding trained staff are set out in our child protection and safeguarding policy as well relevant job descriptions.

A 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, including subject coordinator, 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 regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is 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 an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Support the named contact for online safety incidents (DHT) in ensuring that any online safety incidents are logged on CPOMS 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.

3.5 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)
- Support the named contact for online safety incidents (DHT) in ensuring that any online safety incidents are logged on CPOMS 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
- Ensure that pupils are supervised appropriately whilst using IT equipment and not left unattended whilst online.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- 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 factsheet - Childnet International

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.

4. 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.
From September 2020 **all** schools will have to teach:
- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety.

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

Pupils in **Key Stage 2** 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
- 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.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online; we may also invite speakers to talk to pupils about this. We will also respond to national days/themes such as Anti Bullying Day, Safer Internet Day and Human Rights Day, as well as national issues and situations in the media.

5. 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 covered 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.

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 behaviour policy.)

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. Staff will discuss cyber-bullying with their classes or groups, and the issue will be addressed in assemblies.
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, 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 also sends information/leaflets on cyber-bullying to parents 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 Headteacher or member of the SLT 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, 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.

8. Pupils using mobile devices in school

Year ⅚ pupils may bring mobile devices into school, but are not permitted to use them during school hours. An agreement must be signed by a parent prior to phones being brought into school. Pupils must hand in their phone to a member of staff and then this is kept in the office during the school day. Phones brought into school are done so only to support pupils with their independent journeys to and from school.
Any breach of the mobile phone agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use policy.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB storage devices must not be used. Staff can make use of the cloud storage provided by Google Drive.
If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

Work devices must be used solely for work activities.

10. 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 policies on behaviour and ICT and internet acceptable use. 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.
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).
DSLs 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.

12. Monitoring arrangements

Behaviour and safeguarding issues related to online safety are logged on CPOMS. This policy will be reviewed every 3 years by a DSL. At every review, the policy will be shared with the governing board.

13. 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
- Privacy notice
- Freedom of Information Policy
- Complaints procedure
- ICT and Internet Acceptable Use Policy
- Staff Mobile Phone Policy

Appendix 1: EYFS and KS1 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: ● Ask a teacher or adult if I can do so before using them ● Only use websites that a teacher or adult has told me or allowed me to use ● Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends ● Use school computers for school work only ● I will be kind to others and not upset or be rude to them ● Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends. ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 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:	
I will read and follow the rules in the acceptable use agreement policy **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 another member of school staff) 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 **If I bring a personal mobile phone or other personal electronic device into school:** ● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online ● I will make sure the mobile phone agreement has been signed before I bring it into school, I will hand it into a member of staff for safekeeping in the office during the school day. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
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 for using personal electronic devices in school, and will make sure my child understands these. If my child brings a mobile phone into school, I understand that I must sign the mobile phone agreement first and mobile phones will be handed into a member of staff and kept in the office during the school day.	
Signed (parent/carer):	**Date:**

Appendix 3: 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?	

Acceptable Use Policy For Staff And Volunteers

The computer system (including laptops and mobile devices) is owned by Water Hall Primary School and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's **Acceptable Use Policy** has been drawn up to protect all parties – pupils and staff of the school.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That the schools IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. and
- That staff are protected from potential risk in their use of IT in their everyday work.

Water Hall Primary School will try to ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Water Hall Primary School reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited. Staff should be aware that files and/or hardware will be handed to the Police or law enforcement agency.

Water Hall Primary School reserves the right to amend this Acceptable Use Policy Agreement, at any time. **It is your responsibility to ensure that you are up to date with such changes.**

Acceptable Use Policy Agreement

I understand that I must use the school systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate young people in my care in the safe use of IT and embed Online safety in my work with pupils.

For my professional and personal safety:

1. I understand that Water Hall Primary School will monitor my use of the IT systems, email and other digital communications.

2. I understand that the rules set out in this agreement also apply to the use of school IT systems and equipment when used off-site.

3. I understand that the IT systems are intended for educational use and that I will not use the systems for personal or recreational use.

4. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

5. I will immediately report any illegal, inappropriate or harmful material, website or incident. I become aware of, to the appropriate person.

6. I will be professional in my communications and actions when using the IT systems:
    a. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
    b. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
    c. I understand that email can be forwarded or inadvertently sent to the wrong person, the same levels of language should be applied as for the letters or other media.
    d. I will ensure that when I take and/or publish images of others I do so with their permission and in accordance with the schools policy on the use of digital images/video images. **I will not use**

my personal equipment to record these images. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.

e. I will only use chat and social networking sites in accordance with the schools policies.
f. I will only communicate with pupils and parents using the official systems. Any such communication will be professional in tone and manner.
g. I will not engage in any Online activity that may compromise my professional responsibilities.

7. The school has the responsibility to provide safe and secure access to technologies.
    a. When I use my personal devices (incl phone, handheld, laptop, etc), I will follow the rules set out in this agreement, in the same way as if I was using fixed equipment. I will also follow any additional rules set about such use. I will ensure that any such devices are protected by up to date anti-virus software, are free from viruses and secured via password or PIN code.
    b. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
    c. I will ensure that my data is regularly backed up.
    d. I will not try to upload, download or access any materials which are illegal (child sexual abuse, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
    e. I will not install or attempt to install programmes of any type on a machine, or store programmes on a PC, I will not try to alter computer settings, unless this is allowed in a specific policy.
    f. I will not disable or cause any damage to school equipment, or the equipment belonging to others.
    g. I understand that what is on my device is my responsibility and I am accountable.

8. I will only transport, hold, disclose or share personal information about myself or others as outlined in the schools Data Protection Policy. Where personal data is transferred outside the school network, it must be encrypted.
    a. I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except where it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
    b. I will immediately report any damage or faults involving equipment or software, however this may have happened.

9. When using the internet in my professional capacity:
    a. I will ensure that I have permission to use the original work of others in my own work.
    b. I will adhere to the licensing terms and conditions of software and services
    c. Where work is protected by copyright, I will not download or distribute or save to the school network copies (including music and videos).
    d. I will not break copyright by ripping/converting CDs and DVDs and storing them on the school network.
    e. I will not attempt to access any streaming services that host or distribute copyright material. e.g. Putlocker style sites.

10. I understand that I am responsible for my actions in and out or work:
    a. I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in work, but also applies to my use of school IT systems and equipment out of work and my use of personal equipment in school or in situations related to my employment.
    b. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, dismissal. I understand that all illegal activities will be reported to the Police and relevant law enforcement agencies.

11. I will ensure that any use of social media does not:
    - bring the school into disrepute.
    - breach confidentiality.
    - breach copyrights of any kind.
    - bully, harass or be discriminatory in any way. and
    - cannot be classified as defamatory or derogatory.

Anyone who uses laptops and/or other property from the school will assume all liability and responsibility for safeguarding it while it is loaned out to them.

Please take the following precautions:

- If you leave your laptop in school when not in use, be sure to lock it away securely and do not just leave it out in the classroom or shared spaces.
- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.
- Keep the laptop in your sight when travelling on public transport.
- If you are travelling by car, lock your laptop in the boot when you park.
- Do not use the laptop in locations that might increase the likelihood of damage.
- Keep food and drinks away from the laptop.

If equipment assigned to you is lost, stolen, or damaged and the above guidelines were not followed the user will be liable for the costs of replacement or repair costs at the current market value. The school may also take disciplinary action where it is considered that an act of negligence has led to damage or theft of school-owned equipment.

If you have homeowners insurance, that policy may cover part, or all, of the costs. Teachers should notify their insurance company and have some coverage in that manner.

If there are any problems with IT related equipment the schools IT dept. must be informed. Repairs **MUST NOT** be undertaken by anyone else.

On termination of employment all IT equipment is to be returned to the IT department directly to be checked and then reissued.

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

Print Name: _____

Sign: _____

Date: _____