Walhampton

Walhampton Online Safety Policy

Drafted by:	Head of IT
Approved by:	General Committee
Approval date:	January 2020
Next review date:	January 2021
ISI Policy Nos.:	

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the pupils and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of the school community - staff, pupils , volunteers, parents and carers, visitors, community users - who have access to and are users of the school's ICT systems.

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom and classrooms.

- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by parents at the start of each year.
- Acceptable use agreements to be issued to the whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupils and personnel files.

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school can not accept liability for material accessed, or any consequences of internet access.
- Staff and pupils are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our Head of IT is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Head or Bursar.
- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school child protection procedure.

Review and Monitoring

Online safety is integral to other school policies including the On-line Safety Policy, Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's Head of IT is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and online safety issues in the school.

This policy has been developed in consultation with the school's online safety committee and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

2. Education and Curriculum

Pupil online safety curriculum

The school has a clear, progressive online safety education programme primarily as part

of the Computing curriculum / PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to pupils ' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind pupils about their responsibilities using the Acceptable Use Agreement signed by every pupil or on their behalf by their guardian or parent.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and pupils understand issues around plagiarism and copyright/ intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Staff and governor training

The school will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information. Please refer to the BYOD policy
- Regular training is available to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in school.

- Opportunities to share in their children's online safety learning (eg assemblies, performances).
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3. Conduct and Incident management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school's Misuse Plan. The school actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about pupils .

4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- Each pupil has a single sign log-in and password.
- The administrator passwords for the school ICT system, used by the Network Manager (subcontracted to Medhurst) are also available to the Bursar and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for different ages / stages and different groups of users – staff / pupils .
- The school regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach.
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Social Media

The school has a Social Media Policy that covers the management of school accounts and sets out guidelines for staff personal use of social media.

5. Data

The school has a Data Protection and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer (SIRO); and the storage and access of data.

There is a policy outlining when and how staff may use their own devices for work purposes and this includes the handling of personal data and sensitive information.

6. Equipment and Digital Content

Use of Mobile Technologies

Personal mobile phones and 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 personal mobile phones or mobile devices.

Pupil Use

No day pupils should bring mobile phones or mobile devices into school. Any device brought into school will be confiscated. Permission must be sort from the Head if a parent deems it necessary for a child to have a mobile phone. The phone must be signed in and out of the school office.

The school strongly advises that pupil mobile phones should not be brought into school.

Pupil mobile phones must be turned off / placed on silent and stored out of sight in school. They must remain turned off and out of sight until the end of the day. Mobile phones will not be used during lessons or formal school time unless with consent from a member of staff.

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Boarders may have mobile phones that MUST be kept in the boarding office and only used at permitted times to contact parents at the end of the school day.

Authorised staff can search pupil's electronic devices if they have good reason to think

that the device has been or could be used to cause harm, disrupt teaching or break school rules. Any search will be carried out in line with the school's Search Policy – Electronic Devices.

Staff Use

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

School devices, including mobile phones and cameras, must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day or as soon as possible.

In the Prep department staff personal mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods or when staff are on break and boarding unless permission has been granted by a member of the senior leadership team.

Staff can NOT use their own devices, such as mobile phones or cameras, to take photos or videos of pupils. Images must be taken using a school camera or device. The photos must be stored on the school server or on an authorised photo school portal. In exceptional circumstances, authorisation to do so can be given by the Head or Bursar.

Where staff are required to use a mobile phone for school duties – e.g. in case of emergency during off-site activities, or for contacting pupils or parents - then a school mobile phone will be provided where possible. In an emergency where staff do not have access to a school device, they should use their own device and hide their own number (by dialling 141 first).

Personal mobile phones are **not** to be used by Pre-Prep staff during any contact time with children. Be this in class, the playground, a club or the dining room.

They are to be **switched off** and kept in a closed bag or preferably stored in the staff room.

Should a member of Pre-Prep need to use a phone during the day the school office land line may be used. In exceptional circumstances, the Head of Pre-Prep can give

permission for a personal mobile phone to be used.

When Pre-Prep staff have non-contact time staff may use their mobile phone in the classroom or the staffroom with the door closed.

Digital images and video

We will seek permission from parents and carers for the use of digital photographs or video involving their child as part of the Use of Digital and Video Images Agreement when their child joins the 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.

If specific pupil photos (not group photos) are used on the school website or prospectus we will obtain individual parental or pupil permission for its use.

Pupils are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Pupils understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

Photography and video images play an important part in learning activities and documenting life at school. Pupils and members of staff may use school owned cameras to record activities in school and on school trips.

These images may be used in subsequent lessons, on school display boards, in the school's newsletter and on Firefly. The images may also be published publicly on the school website, on the school's social media channels, in the press and in materials used to promote the work of the school.

The school will comply with the General Data Protection Regulations and ensure that we have parent/carer permission before taking and using images of pupils. We will also ensure that when images are published publicly, pupils cannot be identified by name.

The school has a secure storage system for maintaining our current and archived image libraries. Where a professional photographer is used to take photographs and videos at school, we have contracts in place to ensure photos are stored securely and without name identifiers.

Parents/carers are welcome to take videos and images of their children at school events for their own personal use. To respect others' privacy (and in some cases for protection) images including other children should not be published or made publicly available on social networking sites unless permission has been gained directly from the other child's parents/ carers.

In addition to the general procedures laid out above, the school will keep in mind the following best practices, especially where deliberate misuse is suspected:

- Involve multiple senior members of staff or governors in the review and monitoring process if possible
- Use a designated and secured computer for the duration of the review. The computer should not be one that is used by students and should be one that police can take off-site if needed
- Keep a careful record of any websites and content visited while investigating a misuse incident, including the url of the site and a description of the content in question. In some cases it may be necessary to store screenshots of the content. (Please note that this does **not** include images of child sexual abuse – see below)
- If child abuse images are discovered in the course of a review, internal monitoring should immediately be stopped and the incident should be reported to the police. The police should also be consulted if a review uncovers grooming of a child, obscene material sent to a child, adult material in violation of the Obscene Publications Act, criminally racist material or any other illegal activity.