
# E-safety and Acceptable Use Policy

| Rev | Date | Description |
|---|---|---|
| 2 | 04/10/2016 | Reviewed by safeguarding working group |
| 1 | 01/01/2014 | Initial version |

This policy is part of the school's **child protection and safeguarding policy**. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

# 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 Worple Primary School with respect to the use of IT-based technologies
- Safeguard and protect the children and staff
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community
- Have clear structures to deal with online abuse such as online bullying, in line with the school's **anti-bullying policy**
- 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 children.

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

### Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content.

### Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords.

### Conduct

- Aggressive behaviours (bullying)

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership).

## Scope

This policy applies to all members of the Worple Primary School community (including staff, children, volunteers, parents, carers, visitors and community users) who have access to and are users of the school's IT systems, both in and out of Worple Primary School.

## Roles and responsibilities

| | |
|---|---|
| Designated safeguarding lead | **Donna O'Connor** |
| Designated safeguarding governor | **Rob Kemp** |
| Computing subject lead | **Samia Ahmad** |
| Online safety co-ordinator | **Samia Ahmad** |
| Network manager | **Adam Wignall**<br>adam.wignall@strawberry7.com |
| Data and information (asset owners) managers (IAOs) | **Donna O'Connor** |
| LGfL nominated contact(s) | **Samia Ahmad**<br>**Laureen O'Brien**<br>**Adam Pearce**<br>**Adam Wignall** |
| Local Authority Designated Officers (LADO) | **Hetsie van Rooyen**<br>**Sally Grieg**<br>020 8583 3066<br>cpcc-gcsx@hounslow.gcsx.gov.uk |

| **Role** | **Key Responsibilities** |
|---|---|

| | |
|---|---|
| Head teacher | ● Must be adequately trained in offline and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance<br>● To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.<br>● To take overall responsibility for online safety provision<br>● To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling<br>● To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services<br>● To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles<br>● To be aware of procedures to be followed in the event of a serious online safety incident<br>● Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of children, including risk of children being radicalised<br>● To receive regular monitoring reports from the online safety co-ordinator<br>● To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager<br>● To ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety<br>● To ensure school website includes relevant information. |
| Designated safeguarding lead<br>Computing subject lead | ● Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's e-safety and acceptable use policy<br>● Promote an awareness and commitment to online safety throughout the school community<br>● Ensure that online safety education is embedded within the curriculum<br>● Liaise with school technical staff where appropriate<br>● To communicate regularly with SLT and the safeguarding governors' working group to discuss current issues, review incident logs and filtering or change control logs<br>● To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident<br>● To ensure that online safety incidents are logged as a safeguarding incident<br>● Facilitate training and advice for all staff<br>● Oversee any children's surveys and children's feedback on online safety issues<br>● Liaise with the Local Authority and relevant agencies<br>● Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns. |

| | |
|---|---|
| Safeguarding governor (including online safety) | ● To ensure that the school has in place policies and practices to keep the children and staff safe online<br>● To approve the e-safety and acceptable use policy and review the effectiveness of the policy<br>● To support the school in encouraging parents and the wider community to become engaged in online safety activities<br>● The role of the online safety governor will include: regular review with the online safety co-ordinator. |
| Computing subject lead | ● To oversee the delivery of the online safety element of the computing curriculum |
| Network manager | ● To report online safety related issues that come to their attention, to the online safety co-ordinator<br>● To manage the school's computer systems, ensuring:<br>○ school password policy is strictly adhered to<br>○ systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)<br>○ access controls/encryption exist to protect personal and sensitive information held on school-owned devices<br>○ the school's policy on web filtering is applied and updated on a regular basis<br>● That they keep up to date with the school's e-safety and acceptable use policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant<br>● That the use of school technology and online platforms are regularly monitored and that any misuse or attempted misuse is reported to the online safety co-ordinator or head teacher<br>● To ensure appropriate backup procedures and disaster recovery plans are in place<br>● To keep up-to-date documentation of the school's online security and technical procedures |
| Data and information (asset owners) managers (IAOs) | ● To ensure that the data they manage is accurate and up-to-date<br>● Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.<br>● The school must be registered with Information Commissioner |
| LGfL nominated contact(s) | ● To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant |

| | |
|---|---|
| Teachers | ● To embed online safety in the curriculum<br>● To supervise and guide children carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)<br>● To ensure that children are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws |
| All staff, volunteers and contractors. | ● To read, understand, sign and adhere to the school staff acceptable use agreement, and understand any updates annually. The AUA is signed by new staff on induction.<br>● To report any suspected misuse or problem to the online safety coordinator<br>● To maintain an awareness of current online safety issues and guidance, e.g. through CPD<br>● To model safe, responsible and professional behaviours in their own use of technology |
| **Exit strategy** | ● At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset |
| Children | ● Read, understand, sign and adhere to the children's acceptable use policy annually<br>● To understand the importance of reporting abuse, misuse or access to inappropriate materials<br>● To know what action to take if they or someone they know feels worried or vulnerable when using online technology<br>● To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's e-safety and acceptable use policy covers their actions out of school<br>● To contribute to any 'pupil voice' and surveys that gathers information of their online experiences |
| Parents and carers | ● To read, understand and promote the school's children's acceptable use agreement with their children<br>● to consult with the school if they have any concerns about their children's use of technology<br>● to support the school in promoting online safety and endorse the parents' acceptable use agreement which includes the children's use of the Internet and the school's use of photographic and video images |

| | |
|---|---|
| External groups including Parent groups | • Any external individual or organisation will sign an acceptable use agreement prior to using technology or the Internet within school<br>• to support the school in promoting online safety<br>• To model safe, responsible and positive behaviours in their own use of technology. |

## Communication

The policy will be communicated to staff, children and the community in the following ways:

- Policy to be posted on the school website and staff room
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and children at the start of each year
- Acceptable use agreements to be issued to whole school community, on entry to the school.

## Handling incidents

The school will take all reasonable precautions to ensure online safety.

Staff and children are given information about infringements in use and possible sanctions.

The online safety co-ordinator acts as first point of contact for any incident.

Any suspected online risk or infringement is reported to the online safety co-ordinator that day.

Any concern about staff misuse is always referred directly to the head teacher, unless the concern is about the head teacher in which case the complaint is referred to the chair of governors and the LADO (Local Authority Designated Officer).

## Review and monitoring

The e-safety and acceptable use policy is referenced within other school policies (notably the **child protection and safeguarding policy** and the **anti-bullying policy**).

The e-safety and acceptable use 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. All amendments to the school e-safety and acceptable use policy will be disseminated to all members of staff and children.

# Education and curriculum

## Child online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the computing and PSHE curriculum, which covers a range of skills and behaviours appropriate to their age and experience
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- will remind children about their responsibilities through the children's acceptable use agreement
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging off, use of content, research skills, copyright
- ensures that staff and children understand issues around plagiarism, how to check copyright and also know that they must respect and acknowledge copyright and intellectual property rights
- ensure children only use school-approved systems and publish within appropriately secure or age-appropriate environments.

## Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all new staff, including those on university or college placement and work experience with information and guidance on the e-safety and acceptable use policy and the school's acceptable use agreements.

## Parent awareness and training

This school:

- runs a rolling programme of online safety advice, guidance and training for parents.

# Expected conduct and incident management

## Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant acceptable use agreements

- understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good online safety practice when using digital technologies in and out of school
- know and understand school policies on the use of mobile and handheld devices including cameras.

Staff, volunteers and contractors:

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older children have more flexible access
- know to take professional, reasonable precautions when working with children, previewing websites before use; using age-appropriate (child friendly) search engines where more open Internet searching is required with younger children.

Parents and carers:

- should provide consent for children to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

## Incident management

In this school:

- there is strict monitoring and application of the e-safety and acceptable use policy and a differentiated and appropriate range of sanctions
- all members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible

- the police will be contacted if one of our staff or children receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – police, Internet Watch Foundation and inform the LA.

# Managing IT and communication systems

## Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet and email use is monitored
- has the educational filtered secure broadband connectivity through the LGfL
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming); all changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- uses USO user-level filtering where relevant
- ensures network health through use of Sophos anti-virus software (from LGfL)
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file and email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect children.

## Network management (user access, backup)

This school:

- Uses individual, audited logins for all users - the LGfL USO system
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful
- Has additional local network monitoring/auditing software installed
- Ensures the network manager is up-to-date with LGfL services and policies
- Has daily backup of school data (admin and curriculum)

- Uses secure, cloud storage for data backup that conforms to DfE guidance

**Cloud software services: how schools should protect data**
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

- Storage of all data within the school will conform to the EU and UK data protection requirements
- Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

**EU data protection directive**
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety and acceptable use policy. Following this, they are set-up with Internet, email access and network access.
- All children have access to class logins and individual email usernames and passwords, which gives them access to the Internet and other services.
- Makes clear that no one should log on as another user and makes clear that children should never be allowed to log-on or use teacher and staff logins
- Has set-up the network with a shared work area for children and one for staff. Staff and children are shown how to save work and access work from these areas
- Requires all users to log off when they have finished working or are leaving the computer unattended
- Ensures all equipment owned by the school and/or connected to the network has up-to-date virus protection
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies, e.g. borough email or intranet; finance system, personnel system etc.
- Maintains equipment to ensure health and safety is followed

- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school or LA approved systems
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- Has a clear disaster recovery system in place that includes a secure, remote off-site backup of data
- Uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools
- Ensures that all child level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)
- Has a wireless network that has been secured to industry-standard enterprise security level and appropriate standards suitable for educational use
- Ensures that all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

## Password policy

This school makes it clear that staff and children must always keep their passwords private, must not share with others. If a password is compromised the school should be notified immediately.

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.

We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days.

We require staff using critical systems to use two factor authentication.

## Email

This school:

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear that personal email should be through a separate account;
- Uses anonymous or group email addresses, for example info@schoolname.la.sch.uk, head@schoolname.la.sch.uk, or class email addresses
- Will contact the police if one of our staff or children receives an email that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date

- Uses a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Children:

- Use LGfL pupil email system which are intentionally 'anonymised' for child protection
- Are taught about the online safety and netiquette of using email both in school and at home.

Staff:

- Will use LA or LGfL email systems for professional purposes
- May find access to external personal email accounts be blocked within the school

Staff must never use email to transfer staff- or child-personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data or file must be protected with security encryption.

Email is not a safe way of sending sensitive information. Any document that contains as little as a child's name and the school's name is considered sensitive information. All sensitive information can be securely sent via USO FX, or via an encrypted memory stick, which should be available for all members of staff. Anyone who fails to do this may risk disciplinary action according to the **disciplinary policy**.

## School website

The head teacher, supported by the governing body, takes overall responsibility to ensure that the website's content is accurate and the quality of presentation is maintained.

The school website complies with statutory DfE requirements.

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Photographs published on the web do not have full names attached. We do not use children's names when saving images in the file names or in the tags when publishing to the school website.

## Cloud environments

In a virtual learning environment, photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.

## Social networking

Staff, volunteers and contractors:

- Are instructed to always keep professional and private communication separate

- Are instructed not to run social network spaces for children's use on a personal basis or to open up their own spaces to children, but to use the school's preferred system for such communications
- Will adhere to the staff acceptable use agreement for the use of any school-approved social networking.

School staff will ensure that in private use:

- No reference should be made in social media to children, parents, carers or school staff
- Staff should not be online friends with any child. Any exceptions must be approved by the head teacher
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Children:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Are required to sign and follow our age-appropriate children's acceptable use agreement.

Parents:

- Are reminded about social networking risks and protocols through our parental acceptable use agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

# Data security: management information system access and data transfer

## Strategic and operational practices

At this school:

- The head teacher is the senior information risk officer (SIRO)
- Staff are clear who the key contacts are for key school information (the information asset owners), listed above
- We ensure staff know who to report any incidents where data protection may have been compromised
- All staff are DBS checked and records are held in a single central record.

## Technical solutions

Staff have secure areas on the network to store sensitive files.

We require staff to logout of systems when leaving their computer. Enforcement of an automatic logout after an idle time will be at the head teacher's discretion.

We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.

All servers are in lockable locations and managed by DBS-checked staff.

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

| |
|---|
| **The Waste Electrical and Electronic Equipment Regulations 2006**<br>http://www.legislation.gov.uk/uksi/2006/3289/pdfs/uksi_20063289_en.pdf |
| **The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007**<br>http://www.legislation.gov.uk/uksi/2007/3454/pdfs/uksi_20073454_en.pdf |
| **Electrical waste: retailer and distributor responsibilities**<br>https://www.gov.uk/electricalwaste-producer-supplier-responsibilities |

Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

# Equipment and digital content

## Mobile devices (mobile phones, tablets and other mobile devices)

Mobile devices brought into school are entirely at the staff member, children and parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from head teacher or SLT.

Children's personal mobile devices, which are brought into school, must be turned off (not placed on silent). All mobile devices will be handed in at reception should they be brought into school.

The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.

Personal mobile devices will only be used during lessons with permission from the head teacher.

No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

Staff members may use their phones during school break times.

All visitors are requested to keep their phones on silent.

The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the head teacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the head teacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

The school reserves the right to search the content of any mobile device on the school's premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring. Search processes are conducted in accordance with the **behaviour policy**.

If a child needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permission from the head teacher to use their phone at times other than their break times.

## Storage, syncing and access

### The device is accessed with a school-owned account

The device is accessed with a school-created account and all applications and file use is in line with this policy. No personal elements may be added to this device.

PIN access to the device must always be known by the network manager.

### The device is accessed with a personal account

If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.

PIN access to the device must always be known by the network manager.

Exit process: when the device is returned the staff member must log in with personal ID so that the device can be factory-reset and cleared for reuse.

## Children's use of personal devices

The school strongly advises that children's mobile phones and devices should not be brought into school.

The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

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

Children should protect their phone numbers by only giving them to trusted friends and family members. Children will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

## Staff use of personal devices

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

Staff will be issued with a school phone where contact with children, parents or carers is required, for instance for off-site activities.

Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the head teacher.

Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of children and will only use work-provided equipment for this purpose.

In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for

confidentiality purposes and then report the incident with the head teacher or designated officer.

If a member of staff breaches the school policy then disciplinary action may be taken, according to the **disciplinary policy**.

## Digital images and video

In this school:

- We gain parental and carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter or son joins the school (or annually)
- We do not identify children in online photographic materials or include the full names of children in the credits of any published school-produced video materials and DVDs
- Staff sign the school's acceptable use policy; this includes a clause on the use of mobile phones and personal equipment for taking pictures of children
- If specific photos of children (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual permission from the parent or child for its long term, high profile use
- The school blocks or filters access to social networking sites unless there is a specific approved educational purpose
- Children 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
- Children 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
- Children are taught that they should not post images or videos of others without their permission. The school teaches children about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

# Appendices

Appendix 1: Acceptable use agreement (staff, volunteers and governors)

Appendix 2: Acceptable use agreement (Key Stage 1 children)

Appendix 3: Acceptable use agreement (Key Stage 2 children)

Appendix 4: Acceptable use agreement (parents, including photo/video permission)

# Resources

**Protocol for responding to online safety incidents**
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx

**Handling infringements** (page 23 onwards)
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf

**Prevent: radicalisation and extremism**
https://www.gov.uk/government/publications/prevent-duty-guidance

**Data security: Use of IT systems and data transfer**
https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/data-transfer

**Search and confiscation guidance from DfE**
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Worple Primary School

# Acceptable use agreement (staff, volunteers and governors)

The school has provided ICT equipment for use by staff as an important tool for teaching, learning, and administration of the school. Use of school equipment, by both members of staff and children, is governed at all times by the following policy.

All members of staff have a responsibility to use the school's ICT equipment in a professional, lawful, and ethical manner. Deliberate abuse of the school's equipment may result in disciplinary action (including possible termination), and civil and/or criminal liability.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

## Computer security and data protection

You will be provided with a personal account for accessing the computer system, with your own username and password. As such, **you must not disclose your password to anyone** (with the exception of an ICT technician if appropriate),

You **must not allow a child to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.

If you suspect that your password has been seen by anyone you must change it immediately.

When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.

You **must not** store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the school.

You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school (USO FX).

When publishing or transmitting non-sensitive material outside of the school, you **must** take steps to protect the identity of any child whose parents have requested this.

If you use personal ICT equipment at home for work purposes, you **must** ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.

## Personal use

The school recognises that occasional personal use of the school's ICT equipment is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- **must** comply with all other conditions of this policy as they apply to non-personal use, and all other school policies regarding staff conduct;
- must not interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the ICT system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the school.
- any personal data stored on the school equipment **must not** contain any inappropriate material and **must** be in an area inaccessible to children

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

## Conduct

You **must** at all times conduct your ICT usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Making or receiving calls, texts or emails during teaching time (if you are likely to receive an urgent communication, you should arrange for the office to alert you to its arrival and withdraw from class to receive it).

You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.

You **must not** intentionally damage, disable, or otherwise harm the operation of computers.

## Use of social networking websites and online forums

Staff must take care when using social networking websites such as Facebook or MySpace, even when such use occurs in their own time using their own computer. Social Networking

sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any child to access personal information you post on a social networking site. For the purposes of this policy the term "child" refers to current or past pupils (until they reach adulthood, although care should be taken when considering this). In particular:

- You **must not** add a child to your 'friends list'
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You **must not** contact any child privately via a social networking website, even for school-related purposes.
- You **must** take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff must also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.

You **must not** post any material online that can be clearly linked to the school that may damage the school's reputation.

You must not post any material clearly identifying yourself, another member of staff, or a child, that could potentially be used to embarrass, harass, or defame the subject.

## Use of email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

- Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of emails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for email.
- Email to outside organisations has the same power to create a binding contract as hardcopy documents. Check email as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must**

**not** purchase goods or services on behalf of the school via email without proper authorisation.

- All school email you send must have a signature containing your name, job title and the name of the school.
- Email is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external email address may lead to receipt of unsolicited email containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- You must not send chain letters or unsolicited commercial e-mail (also known as spam).

## Supervision of children's use

Children **must** be supervised at **all** times when using school ICT equipment. When arranging use of ICT facilities for children, you must ensure supervision is available.

Supervising staff are responsible for ensuring that the separate acceptable use agreement for children is enforced.

Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of ICT used by children.

## Privacy

Use of the school ICT system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this policy and applicable laws. This may include remote monitoring of an interactive logon session.

The school may also use measures to audit use of computer systems for performance and diagnostic purposes.

## Confidentiality and copyright

Respect the work and ownership rights of people outside the school, as well as other staff or children.

You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

As per the standard staff contract, any invention, improvement, design, process, information, copyrighted work, trademark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the school shall be immediately disclosed to the school and shall to the extent permitted by law belong to and be the absolute property of the school.

By storing or creating any personal documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

## Reporting breaches of this policy

All members of staff have a duty to ensure this policy is followed. You must report to the designated safeguarding lead:

- any websites accessible from within school that you feel are unsuitable for staff or children's consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a child via the school computer system.

All reports will be treated confidentially.

| | |
|---|---|
| **Full name (printed)** | |
| **Job title/role** | |
| **Signature** | |
| **Date** | |

**Authorised signature (head teacher/assistant head teacher)**

I approve this user to be set-up on the school systems relevant to their role.

| | |
|---|---|
| **Full name (printed)** | |
| **Signature** | |
| **Date** | |

Worple Primary School

# Acceptable use agreement (Key Stage 1 children)

## Think before you click

| | | |
|---|---|---|
| S |  | I will only use the Internet and email with an adult |
| A |  | I will only click on icons and links when I know they are safe |
| F |  | I will only send friendly and polite messages |
| E |  | If I see something I don't like on a screen, I will click on the dolphin and always tell an adult |

| |
|---|
| My name: |
| My signature: |

Worple Primary School

# Acceptable use agreement (Key Stage 2 children)

## I know that I must use ICT safely

- I know that my teacher can watch what I do on the ICT equipment.
- I will treat my username and password like my toothbrush – I will not let anyone else use it, and I will not use theirs.
- I will be aware of stranger danger when I am contacting other people on the internet.
- I will click on the dolphin immediately if I see anything inappropriate or anything that makes me feel uncomfortable and then always tell a teacher.

## I know that I must use ICT responsibly

- I will only put pictures or videos on the Internet from inside the school if I have permission from the school.
- I understand that the school's Internet filter is there to protect me, and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.
- I will only download photos, music or videos onto the ICT equipment if it is related to my school work.

## I know that I must help look after the ICT equipment

- If I have a problem with my ICT equipment, I will tell a teacher immediately so that the problem can be fixed. I won't leave it broken for the next person.
- I will only use programs or apps that are already on the school equipment. If I need a new program or app, I will ask my teacher. I won't try to install it myself.
- I will only change settings on the equipment if the teacher asks me to.

## I know that I must respect others when using ICT

- I will always treat others the same way I would want them to treat me – just as I would in class or the playground. I will not use the equipment to harass or bully anyone.
- I will always be polite online. I appreciate that others may have different opinions.
- I will not take or share pictures or videos of anyone without their permission.

| |
|---|
| Signed |
| Date |

Worple Primary School

# Acceptable use agreement (parents)

**Internet and ICT** As the parent or legal guardian of the child(ren) named below, I grant permission for the school to give my daughter/son access to:

- the Internet at school
- the school's chosen email system
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep children safe and to prevent children from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

**Use of digital images, photography and video** I understand the school has a clear policy on the use of digital images and video and I support this.

I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

**Social networking and media sites** I understand that the school has a clear policy on the use of social networking and media sites and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

| | |
|---|---|
| **My daughter's/son's name** | |
| **Parent's/guardian's signature** | |
| **Date** | |

## The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

- If the child is named, we avoid using their photograph.
- If their photograph is used, we avoid naming the child.

Where showcasing examples of children work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that children aren't referred to by name on the video, and that children's full names aren't given in credits at the end of the film.

Only images of children in suitable dress are used.

Staff members are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian
- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint presentations
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. within a CDROM or DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

**Note** If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

## The use of social networking and online media

This school asks its whole community to promote the the common approaches to online behaviour:

- Common courtesy

- Common decency
- Common sense

## How do we show common courtesy online?

We ask someone's permission before uploading photographs, videos or any other information about them online.

We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

## How do we show common decency online?

We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.

When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

## How do we show common sense online?

We think before we click.

We think before we upload comments, photographs and videos.

We think before we download or forward any materials.

We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.

We make sure we understand changes in use of any web sites we use.

We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, child, parent or carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process.

**CEOP report abuse process**
https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/