

Arundel Church of England Acceptable Use of Internet and Digital Technology Policy

Rationale

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote child achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to world wide resources and research materials
- Educational and cultural exchanges between children world wide
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The statutory computing curriculum requires children to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

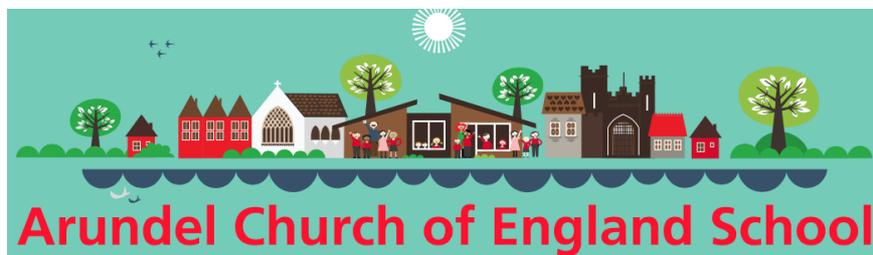
Aims

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following

Acceptable Use Policy.

The Aims of this Acceptable Use Policy are to:-

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and children are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.



General Internet Use and Consent

Children who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Children must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. The school will keep a record which will be regularly referred to by teachers and monitored by the Headteacher. The use of the names of children or photographs of children for websites will require written permission from parent(s)/carer(s) included on the consent form. If a picture is placed on the website the child's name will not be displayed.

Children must not use the school ICT facilities without the supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken Arundel Church of England Primary School and cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or children discover unsuitable sites, the URL (address) and content must be reported to the ICT Leader immediately who will, in turn, record the address and report on to the Headteacher, SBM and Internet Service Provider.

Children are aware that they must only access those services they have been given permission to use. Staff and children are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)

Staff and Governors must agree to and sign the Acceptable Use Agreement (appendix) each year. Children and parent(s)/carer(s) must agree to and sign the Acceptable Use Agreement on entry to the school.

Log in and Passwords

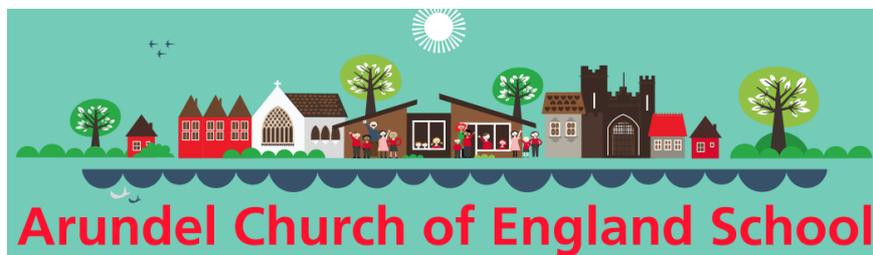
- Children and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.
- Children and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- Staff and children must ensure terminals or lap tops are logged off (or hibernated) when left unattended.

Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each class.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.

Users must treat equipment and services in school and at other sites accessed through school facilities with respect, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities. Risk assessments are completed for use of laptops and laptop trolleys and are kept in the school office. Staff are responsible for sharing the safety issues with their children.



Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day
- People who cyber bully may attempt to remain anonymous
- Anyone of any age can cyber bully
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient

Prevention

We recognize that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided.

We recognize we have a shared responsibility to prevent incidents of cyber bullying but the Headteacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.

Record Keeping and Monitoring Safe Practice

The Headteacher keeps records of cyber bullying. Incidents of cyber bullying will be followed up using Arundel Church Of England's procedures.

E-Safety

E-Safety is recognised as an essential aspect of ICT leadership and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.

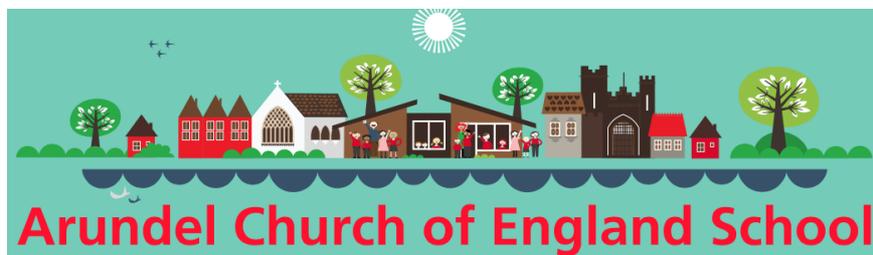
The overall responsibility for E-Safety has been designated to our Headteacher working in conjunction with the ICT coordinator, SBM and Assistant Headteacher.

The ICT Coordinator ensures they keep up to date with E-Safety issues and guidance through liaison with the Local Authority E-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).

All Staff (all teachers, supply staff and teaching partners) are reminded/ updated about E-Safety matters at least once a year and usually more often. Children are regularly informed about e-safety through planned whole school and class assemblies and as an ongoing aspect of the computing curriculum.

Any work or activity on the Internet or school equipment must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.

Staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/children or ex-children) related to the school. Staff



are reminded that any action or comment that brings the school or colleagues into disrepute or compromises child or staff confidentiality will be classed as a disciplinary matter.

Users must not give out personal email or postal addresses, telephone / fax numbers of any person. Under no circumstances give email or postal addresses / telephone numbers / fax numbers of any teachers or children at school.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by children and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

Users must not download, use or upload any material that is subject to copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or

you cannot obtain permission, do not use the material. Users should assume that ALL software is subject to copyright restrictions, including shareware.

Children must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the ICT technician or the ICT Leader before attempting to download or upload software. Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT co-ordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

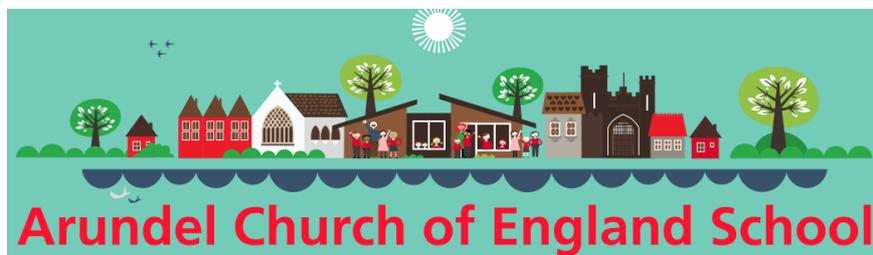
Search engines (such as Google) are not to be used to search for websites or images unless the learning intention specifically demands it.

E-Mail Usage

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

When using e-mail, children and staff should:

- Not access personal emails in school using school equipment
- Be aware that e-mail is not a secure form of communication and therefore children should not send ANY personal information
- Not attach large files
- Not forward e-mail messages onto others unless the sender's permission is first obtained
- Not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive
- Not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated



This Guidance will apply to any inter-computer transaction, be it through web services, chat room, bulletin and news group or peer to peer sharing.

Mobile Devices

Children are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the School Office to look after during the school day and collected at 3.00pm.

Children may not make personal calls or send or receive email or text messages from or to a mobile phone during the school day. Mobile phones may not be used to take pictures of children and staff (use class cameras via ipads provided by the school). Children should not send or receive email or text messages to/from their mobile device during the school day. Any child who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day. Any inappropriate use of mobile devices such as cyber bullying must be reported to the Headteacher.

Staff should only use their mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera. Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

School Network and Child Files

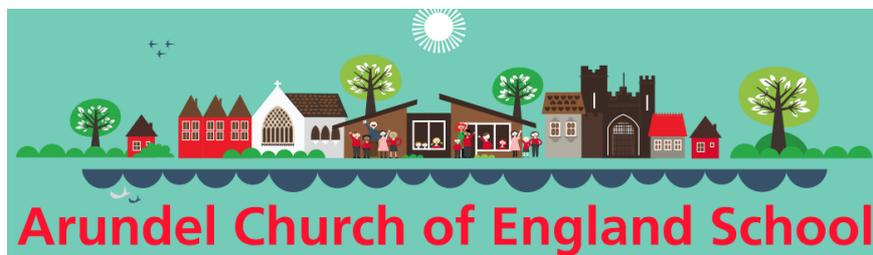
- Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Children can access and save work to their own log-on through the server in the ICT suite as well as dropbox on the trolley laptops or iPads; this can only be accessed by that child, the class teacher, the ICT Coordinator and the ICT technician.

- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT technician will view any material children store on the school's computers, or on memory sticks/disks children use on the school's computers.
- Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network is accessed from home, this Acceptable Use Policy applies.

Network Security Guidelines

Backups

Files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore.



Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost.

Use your Network Area

Always ensure that files are saved to available network/storage area, NOT on the local hard drive. This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Home Documents

The school cannot accept responsibility for personal documents held on school laptops, it is the responsibility of the user to backup documents created at home.

Off site child data and child information

Lap tops and back-ups (USB sticks/external hard drives) may be taken off site. Staff are to ensure that laptops are used cautiously when viewing child data/information and images and that laptops are logged off when left unattended. Images must be transferred to the school network as soon as possible and be removed within the set timescales.

Virus Checks

All computers in school have anti virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician straight away.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT technician to discuss the situation. Solutions are possible! Remember also that shareware is not freeware and must be licensed for continued use.

Under data protection legislation, it is possible to hold and process personal data and/or special category data. Data should be treated with respect, kept confidential and only shared as required for school purposes. There are procedures in place for handling such information and these should be followed. Any person wishing to use the facilities for such a purpose is required to inform the Headteacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at anytime. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.



“Hacking” is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

If children break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Children with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each child. Where a child has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Allegations against Adults Who Work With Children and Young People

Allegations made against a member of staff should be reported to the Senior Designated Officer for safeguarding within the school immediately. In the event of an allegation being made against the Head teacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Additional Information

Please be aware, at such time that you leave Arundel Church of England Primary School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.



If children, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Headteacher for further guidance. This agreement applies to all online use and to anything that may be downloaded or printed.