St. Joseph's Catholic Primary School
'Growing in Faith, Faith in Growing'

Acceptable Use of ICT Policy

2015 / 2016

Acceptable Use of ICT Policy

Contents **Page No.**

E-safety Policy Summary

The following whole-school policy refers to the safe, acceptable and responsible use of the Internet. E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound implementation of e-safety policy in both administration and curriculum.
- Safe and secure broadband from the Walsall Network including the effective management of a filter.
- National Education Network standards and specifications.

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, anti-bullying and for child protection. The school has appointed a named person to co-ordinate e-Safety. This person is Mrs. Barfield, the ICT coordinator. Our e-Safety Policy has been agreed by senior management and approved by governors. The e-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why Internet Use is Important

The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school's Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
Internet usage within the school will always be within the guidance offered by the Child Exploitation and Online Protection Centre (CEOP)

Managing Internet Access

Information system security, School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be reviewed in consultation with Walsall Children's Services. All laptop and tablet devices will be subject to the same security as the school PCs.

E-Mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published Content and the School Web Site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

Pupils' full names will not be used anywhere on the school Learning Platform particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Learning Platform. Pupil's work can only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing

The school will block/filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind, which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing Filtering

The school will work with the Walsall Children's Services, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.If staff or pupils discover an unsuitable site, it must be reported to the named e-Safety person. The ICT Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

Mobile phones should not be used during formal school time. The sending of abusive or inappropriate text messages is forbidden. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Internet Access

All staff will be given the School e-Safety Policy and its importance explained.
All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource. Pupils’ access to the Internet will be under adult supervision at all times. Everyone will be made aware that Internet traffic can be monitored and traced to the individual user through the implementation of forensic software provided by policy central. E-safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored. Parents’ attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site. Parents will be asked to sign and return an Internet access consent form. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Walsall Children’s Services can accept liability for the material accessed, or any consequences of Internet access. The Head Teacher will deal with complaints of Internet misuse. The leadership team undertake an e-safety audit each year to assess whether the e-safety basics are in place.

Acceptable Use Introduction

The Internet is an environment that contains many helpful educational resources, but also many documents, images, and files that may not be suitable. This policy describes what St. Joseph's deems 'acceptable use' of technology for staff and pupils. This policy is intended to protect school systems from any liability incurred by allowing pupils and staff access to the wealth of information on the Internet. This policy applies to all members of the school community (including staff, pupils, students on placement, governors, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

This policy will be used to deal with incidents involving pupils, in conjunction with the school's behaviour, safeguarding and anti-bullying policies where appropriate. The school will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. For incidents involving staff, the school will refer to its disciplinary policy and procedure: any breaches of this acceptable use policy may lead to disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.

Guidelines for children

Internet and device access have been provided to equip children with the necessary resources to build on skills taught in school and at home. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. In order for these to be used safely, staff must encourage children to follow these guidelines: Children must only use computers, devices and the internet when supervised by an adult in school. Children must use school ICT in a responsible way to make sure that there is no risk to the safety of themselves or others. Children must follow and agree to the following guidelines:

Children will be aware that school can monitor their use of ICT systems, email and other device use.

Children will not share their logins or passwords for devices.

Children will be aware of the need to create avatars and nicknames when online so as not to disclose or share their personal photograph and / or name.

Children will be aware that they should not speak to anyone online that they do not know as this can be dangerous.

Children will immediately report any unpleasant or inappropriate material or messages that make them feel uncomfortable.

Children will only use school ICT devices for educational use and not for personal or recreational use unless they have permission to do so.

Children must seek permission before accepting downloads or uploads.

Children must not use school ICT devices for online gambling, internet shopping, video broadcasting or file sharing unless they have the permission of an adult.

Children will respect other pupils' work and will not access, copy, edit or remove any files that do not belong to them.

Children will only use personal "bring your own" devices (phones, USB sticks, etc.) in school with the permission of their class teacher and Head Teacher. If children are using their own devices, they are to follow all the rules set out in this policy. Children will not be able to access social media sites on their home devices in school.

Children must report any damaged devices to their class teacher who will report and log the problem to the ICT coordinator.

Children will not use programs or software that will enable them to bypass the School's filtering systems.

Children will not open any attachments to emails, unless they know the sender.

When using the internet for research, children must ensure that they recognise copyright protection.

Children must understand that ICT must be used appropriately out of school.

Children must be aware that school may take action against them and inform their parents / carers if they are involved in incidents of inappropriate behaviour when they are out of school. Examples of this would be cyber bullying, use of images or personal information, inappropriate comments about school or other pupils on social media sites.

Children not complying to these guidelines may risk losing the right to use ICT devices in school and staff will make parents aware of the reasons for this.

School Computer Network

Any websites visited must comply with school restrictions. If staff or children are offended by content then this must be reported. Staff may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations. Staff may not use the internet to view illegal or seditious material that would place the member of staff or school at legal risk. If wanting to add or download software to be used on the school network, the ICT coordinator must first be informed. Chat rooms are not to be used at any time on the school network. Uploading of material to the internet for use other than work related is not allowed. The purchasing of school related resources over the internet for school purposes should be cleared by the subject coordinator first and is subject to the same authorisation procedures and limits as purchases made by other means. The school network must not be used to hold or process personal data except within the provisions of the Data Protection Act 1984. It should be noted that authorised staff have the ability to access all user files, including email stored on central servers and data on individual computers as well as on the network.

Password Guidelines

We make it clear that staff and pupils must always keep their passwords private, must not share them with others and must not leave them written down where they can be found. All staff and pupils have their own unique username and password to access school systems. They are responsible for keeping passwords private. We require the use of STRONG passwords for access into our MIS Systems. We require staff to change their passwords into the MIS, email and school management systems twice a year.

Electronic Communication for Staff

At St. Joseph's we take advantage from electronic communication. Emails are a permanent document and even when deleted can be retrieved from system backups. A school email address is for school use only and should therefore not be used for personal reasons. In the interest of protecting the safety of staff members, the following guidelines should be adhered to:

When you do not know the person, remain with formal modes of address - use the form Dear Mr / Mrs, etc. and end the email with Regards, Best Wishes.

Increasingly, parents are communicating with staff via email. When there is a need to reply and where this is preferable to a phone call, staff should CC the Head Teacher and Phase Leader in to the reply. Staff should ensure they put as much thought as possible in to the reply and make sure it is grammatically accurate before sending. It might be worth asking a colleague for their opinion before hitting the SEND button.

If the email is confidential, ensure this is marked clearly. You may want to incorporate a disclaimer as a footnote / signature such as the following:

'The information in this email is confidential and may be legally privileged. It is intended solely for the addressee(s). Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying or distribution is prohibited and may be unlawful.'

Do not use copyright-protected material without proper authorisation. To do so is illegal.

When replying to an email, which has been sent to other people as well, take care to reply to the author. Only select the 'Reply to all' if it is really necessary that everyone else should see your reply.

Ensure you have an email signature. It should contain your name, title, school address and telephone number.

Check your email regularly. If you are absent from school for a period of time, ensure you have set up an automatic reply to explain your absence.

If you receive junk mail, delete it straight away and do not reply. If you feel it is appropriate, use the Block Sender option.

If you receive an attachment from an unknown sender, which you are not comfortable with, delete it straight away in the case of viruses and do not open or forward to others.

If you are printing out confidential emails, ensure you collect them straight away from the printer.
If you have enabled the facility on your Smartphone to receive and send emails, ensure your phone has a code / lock in case it gets in to the wrong hands.
Before sending please check the recipient is who you want it to be. The sending of confidential items to the wrong recipient (and some people have the same name) is a breach of the Data Protection Act.

Social Media

For the purposes of this policy, social media includes (but is not limited to) internet forums, blogs, wikis, podcasts, photograph websites, Facebook and Twitter. Staff should follow these guidelines in relation to any social media sites / apps that they use, both in work and in their personal lives. These guidelines apply to all staff working at St. Joseph's. This includes all teachers, teaching assistants, dinnertime staff, site staff, administrative staff, governors, students on placement and volunteers. The reason for this policy is to protect the safety and integrity of staff and to assist those working with pupils to work safely and responsibly. Furthermore, it sets out to offer a code of practice relevant to social media for professional and personal use, as it is important that staff understand how to separate and differentiate between the two. Staff should not access social media sites from the school's computers or other school device when working in school unless it is used for educational purposes, and is previously agreed and sanctioned by the Head Teacher. Staff should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.
Any use of social media should not:

- Bring the school in to disrepute
- Breach confidentiality
- Breach copyrights
- Bully, harass or discriminate
- Be derogatory to others or about others

The school appreciates that people will make use of social media in a personal capacity.
Staff must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to affect the reputation of the school.
When using social media sites, staff should not share login or password details with others.
If using social media sites/apps on your phone ensure you have a lock / pin code to protect entry to your phone.
Keep personal mobile and home numbers private
Staff should restrict access on their social media sites and pages by amending privacy settings. Staff should check their privacy settings regularly, as they can be changed by the social media site from time to time.

There should be no online dialogue between staff and pupils of the school.
Staff should not make 'friends' of pupils at school. If a pupil approaches a member of staff via their social media account, wishing to either 'follow' them or be their 'friend', the staff member should politely refuse or block this. Ideally, this action should then be explained to the child in school, making reference to the inappropriateness of such a connection. Staff should also not make 'friends' of pupils' parents/carers. If such an approach is made the staff member should politely refuse or block this. Ideally, this action should then be explained to the parent / carer either face to face or by telephone, making reference to the inappropriateness of such a connection and potential risks to their employment status.

The use of Twitter for private use is extremely beneficial for CPD purposes. Personal accounts must remain so and there must be an understanding that they will reflect upon a staff member's professionalism and therefore impact on a school's reputation. Staff should remember that nothing should be written that they would not mind repeating in front of a colleague, parent, governor or Head Teacher. It is encouraged that staff will stipulate on their account that the views are personal and not of their employers.
School Twitter accounts will be set with the 'Protect my tweets' box checked, so that other people must make a request to be a follower. Staff members with responsibility for a school Twitter account must check each request to make sure that the follower is appropriate, e.g. does not have inappropriate material on their own timeline, and accept or decline the request to follow accordingly.
Photographs should be taken using school devices (cameras, iPod touches, iPads).
Photographs should not be taken or stored on personal devices (phones, iPods, etc).

If children are tweeting messages from the School Twitter account, ensure an adult checks these before they are sent.
It is helpful to occasionally retweet content from other Twitter users. However, be careful that the site / blog / tweet that you are retweeting is entirely suitable for your audience.

E-safety in school
E-safety should be a constant focus in all areas of the curriculum and staff should reinforce e-safety messages at all times. In lessons where internet use is planned, staff should endeavour to check sites beforehand to determine their suitability for use. Staff should ensure that they are vigilant in monitoring content of the websites that children visit. It is accepted that at times, especially in UKS2, children may need to research topics (e.g. racism, discrimination, drugs, alcohol, social media) that may result in sites being blocked. Staff can request that a site is temporarily accessed for the period of study time needed. Any request must be made with clear reasons for the need.
Pupils should be provided with constant reminders of being critically aware of materials / content that they access online.

Pupils should be encouraged to acknowledge sources of information used and to respect copyright when using material that has been accessed online.
Parents / Carers should be provided with guidance via the school website highlighting good practice for encouraging ‘e-safe’ children.

Blogging
Whilst blogging has been around for 10+ years, more and more schools are now giving their pupils a voice and an audience through blogging. These are mainly in the form of class blogs but can also be in the form of project blogs or individual pupil blogs.
A successful blog can:

- Safely give your pupils a wider audience for their learning.
- Encourage reluctant learners to participate and succeed
- Allow pupils to receive feedback safely from many different people
- Allow your pupils to peer assess each other's learning
- Encourage parental engagement
- Provide a platform that you can embed Web2.0/3.0 tools into
- Promote your pupils' learning across the globe

Blog Rules:
Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilst blogging.
Don'ts:

- Never give away any personal information about your location or identity.
- Don't post pictures of yourself without specific permission from your teacher or parents.
- Never give out your log in details to anyone.
- Don't use text language in your posts

Do's:

- Post about whatever you like.
- If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
- Comment on other people's posts too. Blogging is about commenting and posting!
- If your post doesn't appear straight away, you teacher might be busy, do be patient.
- Try to post about things that your audience would like to read.
- If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
- Do visit other class blogs regularly to read and comment. This helps people come back to your blog.

- Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
- Always tag your posts with your first name and include key words specific to your post.

Use of digital and video images

Digital and video images have created significant benefits to learning. Staff, pupils and Parents / Carers must be aware of the risks associated with sharing images and videos on the internet.

Staff and pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs that are published on the school website or elsewhere (e.g. Twitter) should be carefully selected and should only include initials of pupils.

Written permissions from Parents / Carers will be obtained as part of the admissions procedure and will be held in school. It is each staff member's responsibility to ensure that s/he checks this information and so does not publish photos or videos of these children.

If staff are completing work for external sources for their own CPD (e.g. research projects, management courses, etc.), staff must request parental permission outlining where and why the photo or video is being used.

Use of Mobile Phones and Digital Photography Policy

Children are not allowed to have mobile phones in school. If children bring a phone to school they should take it to the school office where it will be kept until the end of the school day.

Children have their photographs taken to provide evidence of their achievements for their development records (The Early Years Foundation Stage, EYFS 2007).

Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.

Procedures

- Under the data protection act of 1998 school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school network which is pass word protected until the school ceases to operate, should this occur then all photographs will be shredded or deleted from the school network.

- The school's digital cameras must not leave the school setting (unless on an educational visit).

- Photographs are printed in the setting by staff and images are then removed from the camera memory.

- Photographs of children may be taken and used in accordance with parental consent obtained via the Media Permission Form.

- Often photographs may contain other children in the background.

- Events such as Sports Day, outings, Christmas and fundraising events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending.

- Parents must not post photographs or video containing other children on social media websites.

- Many mobile phones have inbuilt cameras so staff mobile phones must not be used to take pictures of children in our school.

- Visitors may only use their phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing children.

- The use of cameras and mobile phones are prohibited in toilets.

- Staff are asked not to make personal calls during their working hours. However in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Head Teacher.

- All school cameras and videos should be kept securely at all times and used with appropriate authority.

Parent / Carer acceptable use policy

Parents are to be made aware that children must be responsible when using the internet and other communications technologies at school and at home.
Parents / Carers will be issued with a notice when their child starts at the school, which outlines the use of the internet and ICT devices in school.
Parents / Carers to be aware that their child will have had to sign an Acceptable Use Agreement in school.
Parents / Carers to understand that children will be receiving e-safety education in school appropriate to their child's age and that staff will be following government guidance on this.
Parents / Carers will be aware that the school will take all necessary precautions to ensure that monitoring and filtering systems are in place.
Parents / Carers to understand that, although staff will take all necessary precautions, school cannot ultimately be held responsible for the nature and content

of materials that may be accessed on school devices.
Parents / Carers to understand that their child’s activity will be monitored and that staff will contact them should there be a deliberate breach of the Acceptable Use Policy.
Parents / Carers must be encouraged to role model safe use of the internet and devices at home and will inform school if they have concerns over their child’s internet usage.
Parents / Carers taking photographs or videos at school events, e.g. concerts, sports days, etc. should not publish these on any social networking site if they contain images of any other children but their own.

Dealing with incidents of online bullying / inappropriate use of social networking sites

Parents / Carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.
The school’s Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.
In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.
The Governing Body understands that, “There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged.” Furthermore, “Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (an individual) to hatred, ridicule or contempt
- cause (an individual) to be shunned or avoided
- lower (an individual’s) standing in the estimation of right-thinking members of society or
- disparage (an individual in their) business, trade, office or profession.” (National Association of Headteachers)

Parents should make complaints through official school channels rather than posting them on social networking sites. Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

Example Letter Regarding Inappropriate Use of Social Networking Site

Dear Mr/Mrs……………..

It has come to the attention of the Governing Body that inappropriate comments regarding the school/members of the school community have been made on a social networking site.

As these comments do not comply with the expectations set out in the school’s Social Networking Policy you are respectfully asked to remove them from the website.

We would encourage you to enter into productive communication with the school in order to resolve any outstanding differences. The school has an ‘open door’ policy with regard to dealing with parental communication and there are also policies in place such as the
Complaints Policy if required.

Yours sincerely

Chair of Governing Body

Asset Disposal

Details of all school-owned hardware and software will be recorded in an ICT inventory.
All redundant equipment will be disposed of through an authorized agency. This will include a written assurance regarding the acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media wiped, if the storage media has failed, it will be physically destroyed.
All disposals of equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment Regulations (Amendment) 2007

Further information can be found on the Environment Agency website.

Staff Tablet Device User Agreement

At all times any such device shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and Email.

These are school devices and therefore are for professional use.

St. Joseph's reserve the right to require the return of tablets from staff members at any time and without notice. If return is requested, it must be handed in within 24 hours of the request being made.

Staff issued with a tablet device are expected to exercise the same care in respect of the security and upkeep of the device as if it were the employee's own property. In particular, it is the employee's responsibility to ensure that their allocated device is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the device in a meeting room or any off-site venue and whilst travelling. Tablets must not be left unattended in motor vehicles at any time.

The device must always be kept and used within the case issued with it.

The pass code for the device will be set up by the school before issue to a member of staff. This pass code must not be changed.

Any device must never be checked in as baggage on an aircraft and must always be taken on board as hand luggage.

The employee should report malfunctions or any other technical problem with the device immediately to a member of SMT, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible. Under no circumstances is the employee to organise repairs to the device before reporting the problem.

Shared use of a tablet by colleagues of the employee to whom it has been issued is permitted, provided the employee concerned is satisfied the colleague(s) in question is / are competent to use the device in a safe and professional manner.

Lending the device to any third party is strictly prohibited. Use of an organisation-owned tablet by the employee's friends and / or family is also strictly prohibited.

Careless loss, damage or misuse of the tablet, its case, wireless keyboard or any other associated peripheral may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.

Specific Apps will be required to ensure maximum functionality of any tablet issued to an employee. Certain Apps will be mandatory and an employee issued with an tablet will be updated from time to time as to the downloading of mandatory Apps.

Staff are able to log in with their own ID and download their own Apps for use in school. However, any Apps, which would benefit other members of staff, can be requested via email to the ICT coordinator who will be responsible for the budget.

Staff should note that the school, via its web management system, can see what Apps are installed on each iPad.

I accept all of the above points

Signed: Name:

Date: Make / Model: Serial No:

Staff Laptop User Agreement

At all times any such laptop shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and Email.

These are school devices and therefore are for professional use.

St Joseph's reserves the right to require the return of the laptop from the staff member at any time and without notice. If return of the laptop is requested, it must be handed in within 24 hours of the request being made.

Staff issued with a laptop are expected to exercise the same care in respect of the security and upkeep of the laptop as if it were the employee's own property. In particular, it is the employee's responsibility to ensure that their allocated laptop is securely locked away at night, whether at work or at home.

Similar care must be taken when leaving the laptop in a meeting room or any off-site venue and whilst travelling. Laptops must not be left unattended in motor vehicles at any time.

A laptop must never be checked in as baggage on an aircraft and must always be taken on board as hand luggage.

The employee should report malfunctions or any other technical problem with the laptop immediately to a member of SMT, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible. Under no circumstances is the employee to organize repairs to the laptop before reporting the problem.

Shared use of an laptop by colleagues of the employee to whom it has been issued is permitted, provided the employee concerned is satisfied the colleague(s) in question is/are competent to use the laptop in a safe and professional manner.

Lending the laptop to any third party is strictly prohibited. Use of an organisation-owned laptop by the employee's friends and/or family is also strictly prohibited.

Careless loss, damage or misuse of the laptop or any associated peripheral may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.

Specific software will be required to ensure maximum functionality of any laptop issued to an employee. The school's technician will install this. Any other software should not be installed or downloaded without prior consultation with the school's technician and ICT co-ordinator.

Staff may not use school laptops to view illegal or seditious material (in school or elsewhere) on the internet that would place the member of staff or school at legal risk.

I accept all of the above points

Signed: Name:

Date: Make/Model: Serial No:

Any employee requiring further information about this policy should contact the Head Teacher

Notice to Parents / Carers regarding Acceptable Use of ICT

At school, we provide children with access to the Internet using a range of devices, such as computers, iPads, tablets, etc. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

Parents / Carers should note that:

Children must be responsible when using the internet and other communications technologies at school and at home.

Children use devices and the internet in school.

Children receive e-safety education in school appropriate to their age; staff follow government guidance on this.

School will take all necessary precautions to ensure that monitoring and filtering systems are in place. However, school cannot be ultimately responsible for the nature and content of materials that may be accessed.

Children's activity will be monitored and a member of staff will contact me should there be a deliberate breach of the school's Acceptable Use Policy.

They should ensure that they role model safe use of the internet on devices at home and inform school if they have concerns over their child(ren)'s internet usage.

Children sign an Acceptable Use Agreement in school.

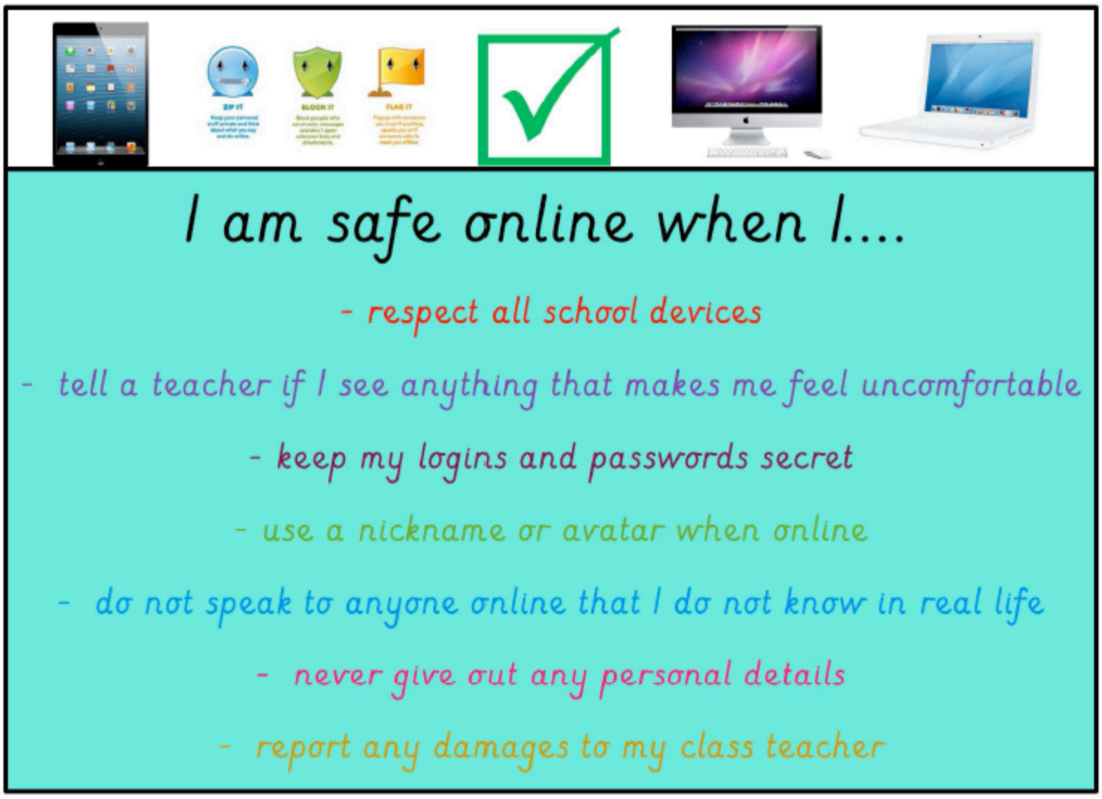
The legal minimum age for having a Facebook account is 13. This is similar to other social media accounts as children below this age are not always aware of the impact of their messages.

Any photographs or videos that parents / Carers take at school events, e.g. concerts, sports days, etc. should not be published on any social networking site if they contain images of any other children but their own.

Unless we are notified by parents / Carers to the contrary, we will assume that they are happy with their child(ren)'s use of the internet and devices within school.

Pupil e-Safety Agreement

Each class teacher will share this agreement with their class at the beginning of each school year, gaining pupils' signatures around it to say that they understand and agree to it. These signed agreements will then be displayed in the classrooms as a visual reminder.



I am safe online when I....

- respect all school devices
- tell a teacher if I see anything that makes me feel uncomfortable
- keep my logins and passwords secret
- use a nickname or avatar when online
- do not speak to anyone online that I do not know in real life
- never give out any personal details
- report any damages to my class teacher