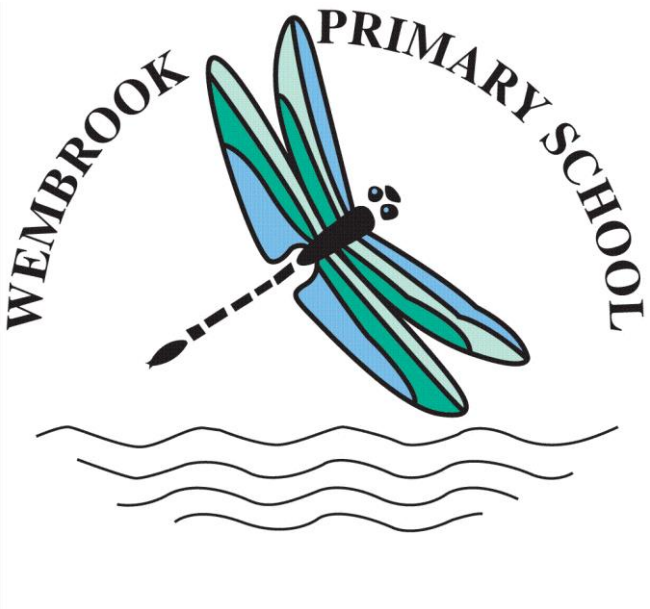
E-Safety Policy



Signed:

Headteacher _____ _____

Chair of Governors _____ _____

E-Safety Policy

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 schools including all staff and students, as well as parents, governors and advisers; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Warwickshire Broadband including the effective management of Websense filtering and Policy Central monitoring.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for Computing and for child protection.

- The e-Safety Coordinator is the Headteacher although he will liaise closely with the ICT coordinator and the ICT administrator. The Headteacher is also the Designated Child Protection Coordinator.
- Our e-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance.

Teaching and learning

The Internet

- The Internet is an essential element in 21st century life 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 Internet access is designed expressly 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- Pupils use the internet widely outside of the school environment and need to learn how to evaluate internet information ensuring that they keep themselves safe.
- In the Computing curriculum, there is an emphasis on teaching pupils about reliability and bias. They should be made aware that anyone can publish online, including those with extremist or inappropriate views.

Managing Internet Access

- The security of the school information systems will be reviewed regularly. Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety officer (see appendices for forms and details of procedures).

E-mail

- Pupils may only use welearn365.com e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail. (see appendices for details of procedures)
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- Staff should consider the wording and content of e-mails sent to external organisations in the same way as a letter written on school headed paper.

The School Website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Teachers should ensure that only photographs of pupils for whom we have parental permission are submitted for use on the website. Photographs of work should not contain pupils' full names.

Social networking and personal publishing

- Social networking sites and newsgroups will be completely blocked for pupils. Staff may use social networking sites or simulated versions for the teaching of e-safety units.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- All staff are strongly discouraged from referencing school in any way on social networking websites.
- Parents are informed via newsletters that it is not appropriate for them to post photographs of school events, which include other pupils in the images, on any social networking website. If they do, the school will request their removal.
- For official class Twitter accounts, separate permission slips must be obtained from parents.

Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Before asking children to complete an internet search, staff should pre-check the links and images brought up by those search terms in case of unsuitable content.

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All users must read and abide by the acceptable ICT use policy before using any school ICT resource (see Appendix 1).
- Parents will be asked to sign and return a consent form which can be found in each pupil's linkbook (see Appendix 2)
- All visitors to the school site who require school network or Internet access, will be asked to read and sign an Acceptable Use Policy.

Assessing risks

- In common with other media, such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 WCC can accept liability for the material accessed, or any consequences of Internet access.
- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Prevent Duty (See separate policy for more detail)

As part of Wembrook Primary School's ongoing safeguarding and child protection duties, we support the Prevent Strategy.

From 1st July 2015, all schools are subject to a duty under Section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent Duty for Schools.

- At Wembrook, we build pupils' resilience to radicalisation by promoting fundamental British Values and enabling our pupils to challenge extremist views.
- The school will work in partnership with the Warwickshire ICT Development Service, to ensure monitoring and filtering systems are as effective as possible in identifying when a pupil is attempting to access sensitive material.
- Where staff, pupils or visitors find unblocked extremist content, they must report it immediately to the ICT Department for action, with screenshots, following the schools official procedures (see appendices for forms and details of procedures).
- The e-safety and Internet user policy refers to preventing radicalisation and related extremist content. Pupils and staff know how to report internet content that is upsetting, inappropriate or of concern.
- There will be cross-curricular links made between the Computing curriculum and the Spiritual, Moral, Social and Cultural Development curriculum.

Handling e-safety complaints

- All disclosures about breaches in E-safety are shared between the Headteacher and the ICT administrator.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher who should use the agreed WCC procedures.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- The school will inform parents/carers of any incidents of concerns, as and when required.

Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

Learning Platform

- The usage of the Learning Platform by pupils and staff will be regularly monitored in all areas, in particular message and communication tools and publishing facilities.
- There is a facility for collaboration within the 'Groups' section of Welearn365 Learning Platform. This is on a secure server, which only welearn365 current users can access. Staff should be mindful of this, monitor groups their pupils use and remind pupils of key safety messages when they communicate with others online.
- Only members of the current pupil, parent/carers and staff community will have access to the Learning Platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.

Mobile Phones/Personal Devices

- Staff should not use personal devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose. In exceptional circumstances, permission must be sought from the Headteacher before use.
- IPads provided by the school may be used to take photographs and videos of pupils. However, these should be uploaded onto the school system and deleted off the iPad on a weekly basis.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Personal data sent over the Internet or taken off site should be encrypted. Use the school e-mail system or One Drive in 'My Area' on the Learning Platform to do this.
- Memory sticks or external hard drives should not be used to store personal data about pupils.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and risks before use in school is allowed.

Communications Policy

- Rules for Internet access/ e-safety guidelines will be posted in all networked rooms (see Appendix 3)
- Pupils will be informed that Internet use will be monitored.
- Safe and responsible use of the Internet and technology for pupils will be reinforced across the curriculum and subject areas. Guidance will be shared with parents to encourage consistency between home and school.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Individual Computing Devices

- Meetings will be held with parents, giving information about the initiative, and detailing e-safety information about our filtering service and monitoring software.
- All pupils and parents will sign an agreement, which details the schools expectations and rules of usage.
- All pupils and parents will sign a separate e-Safety agreement before the child is able to take the device home.

Passwords

All children are provided with an individual username to be used to access the school network. Passwords need to be set before first use:

- Key Stage 1 – a class password may be used for convenience.
- Key Stage 2 – children must choose their own passwords. They should be encouraged to choose a password which cannot be easily identified and contain numbers and letters.

When individual passwords are used, either in Key Stage 1 or Key Stage 2, a record should be kept securely and not made publically visible.

All teaching and support staff are able to change pupil's passwords if needed by going to 'Shared →Staff only →Reset password – Home'
Staff passwords can only be changed by Jo Webb.

Appendix 1: Acceptable Use Policy to be signed by all staff

Warwickshire County Council

WARWICKSHIRE SCHOOL ACCEPTABLE USE POLICY

1. INTRODUCTION

1.1 The internet and e-mail play an essential role in the conduct of our business in school. The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

1.2 How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail and the internet.

1.3 We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

1.4 For your safety, we are able to monitor all web pages visited, email sent and received. This helps us monitor inappropriate use, such as bullying.

1.5 This policy applies to you as an employee whatever your position, whether you are a Head Teacher, Teacher, support staff, permanent, temporary or otherwise. Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

1.6 It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

2. GENERAL PRINCIPLES AND LEGAL ISSUES

2.1 All information relating to our pupils, parents and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically.

2.2 Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

2.3 We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school identifying your school.

2.4 The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

2.5 Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.

2.6 As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

2.7 All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

3. MONITORING COMMUNICATIONS

3.1 This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

3.1.1 to establish the existence of facts

3.1.2 to ascertain compliance with applicable regulatory or self regulatory practices or procedures.

3.1.3 to ascertain or demonstrate effective system operation technically and by users.

3.1.4 for national security/crime prevention or detection.

3.1.5 for confidential counselling/support services.

3.1.6 for Investigating or detecting unauthorized use of the system

3.1.7 for monitoring communications for the purpose of determining whether they are communications relevant to the business.

3.2 Warwickshire LA has an obligation to monitor the use of the internet and e-mail services provided as part of the Warwickshire Broadband service to schools, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. Warwickshire LA and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications

3.3 If the email is personal, it is good practice to use the word `personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

3.4 Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

3.4.1 providing evidence of business transactions;

3.4.2 making sure the School's business procedures are adhered to;

3.4.3 training and monitoring standards of service;

3.4.4 preventing or detecting unauthorised use of the communications systems or criminal activities.

3.4.5 maintaining the effective operation of communication systems.

4. USE OF INTERNET AND INTRANET

4.1 When entering an internet site, always read and comply with the terms and conditions governing its use.

4.2 Do not download any images, text or material which is copyright protected without the appropriate authorisation.

4.3 Do not download any images, text or material which is inappropriate or likely to cause offence.

4.4 If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible. They should check that the source is safe and appropriately licensed.

4.5 If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of the School.

4.6 You are expressly prohibited from:
4.6.1 introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
4.6.2 seeking to gain access to restricted areas of the network;
4.6.3 knowingly seeking to access data which you are not authorised to view;
4.6.4 introducing any form of computer viruses;
4.6.5 carrying out other hacking activities.
4.7 For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
4.7.1 unauthorized access to computer material i.e. hacking;
4.7.2 unauthorized modification of computer material;
4.7.3 unauthorized access with intent to commit/facilitate the commission of further offences.

5.USE OF ELECTRONIC MAIL

5.1 You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
5.2 Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is `Confidential@ in the subject line
5.3 Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
5.4 Do not impersonate any other person when using e-mail or amend any messages received.
5.5 It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

6. DATA PROTECTION

6.1 Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must:
6.1.1 keep the data private and confidential and you must not disclose information to any other person unless authorized to do so. If in doubt ask your Head Teacher or line manager;
6.1.2 familiarize yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
6.1.3 familiarize yourself with all appropriate School policies and procedures;
6.1.4 not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.
6.2 The School views any breach of the Data Protection Act 1998 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.
6.3 If you make or encourage another person to make an unauthorized disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the School may amend this policy from time to time and that I will be issued with an amended copy.

Signed: .....

PRINT NAME: .....

Dated: .....

Appendix 2: Acceptable Use Policy for Pupils/Netbook Users

Pupil E-Safety Agreement Form

Keeping Safe: Stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.
I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, they may contact my parent / guardian.

Pupil's signature _____

For Parents of pupils at Wembrook Primary

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet and other ICT facilities at school.
I know that my daughter / son has signed an e-safety agreement form and that they have agreed to follow the rules for responsible ICT use.
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 will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice and teaching e-safety skills to pupils.

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

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: _____
……

To help the school plan for future initiatives could you please tick the boxes below to indicate what facilities you have at home.

Access to a computer ☐ **Access to Internet** ☐ **Access to Broadband** ☐

Appendix 3: Internet rules displayed in classrooms

S

Be Safe

Keep your personal information safe and secret. Think carefully before you share a photo of yourself or your friends.

Full Name	James Smith
Address	24 Round Street
Phone Number	0121 234 5678
Mobile Number	07777 123456
Email address	jamessmith@myemail.com
School Name	Friendly School
Password	jamesrules

M

Don't Meet Up

Never arrange to meet an online friend because it can be dangerous. No matter how well you think you know people, they might be pretending.

A

Accepting Emails can be dangerous

If you receive junk mail (called spam) or messages that make you feel uncomfortable, tell an adult that you trust and delete them. Don't reply to them.

R

Reliable?

The Internet is full of friendly people and amazing information. However, sometimes people might say or write things which are untrue, so you should always think carefully before trusting what you see or hear.

?

T

Tell Someone!

Most of the time that you are online, you will have lots of fun. However, if you see anything that makes you feel uncomfortable or worried, make sure that you tell an adult that you trust.

Appendix 4: School Procedures

Wembrook Primary School - Dealing with E-Safety Incidents

E-safety school procedures

If any e-safety incidents arise, please complete a 'Pupils E-Safety Incident Form'. Copies of this can be found in the ICT Suite or in the Shared Area, under E-Safety. This form, along with a screen shot if possible, should be returned to Jo Webb/Connor Edgington immediately. If the incident has occurred on a netbook or iPad, also send the device to the ICT Office. This applies whether the incident was deliberate or accidental.

Offensive e-mails

Children should be encouraged to report offensive e-mail content to an adult. Ensure the e-mails in question are not deleted and report the matter to Jo or Connor so that the trail can be investigated.

Unsuitable web content

Make children aware that, if they see something which upsets them, they should not shut down the computer. Instead, they should turn off the screen or close the lid of a laptop and inform an adult. This helps us to capture the evidence needed. Send for Jo or Connor . If they are not available immediately, take a screenshot of the incident, record the computer name eg. WEM-ICT-204, and complete a 'Pupils E-Safety Incident Form'.

If any staff are searching the internet in front of children, ensure you have checked beforehand that the results are suitable. If you are carrying out an ad-hoc search during a lesson, particularly an image search, freeze your whiteboard so you can check the results before the children see.
If an adult discovers any inappropriate web content, please note down full details of the search terms or web address and report these to Jo or Connor.

External adults

If you have any students, work experience placements, volunteers or other adults within your classroom, they should not be using the computers under any staff member's log-on. Instead, inform Jo and she will arrange a guest log-on for them and ask them to sign an Acceptable Use Policy. These guest log-ons have more permissions than the children's log-ons but not full staff access rights.

Appendix 5: E-Safety Incidents Form

Pupils E-Safety Incidents Name: _____ Date:_____

Description of incident and a screen shot (press print screen and paste into an office document.)

Computer location and name (e.g. ICT suite Computer number WEM-ICT-224):

_____

Incidents	Refer to Headteacher	Refer to Police	Refer to ICT Technician	Inform parents/ careers	Removal of network/internet access	Warning	Further sanctions e.g. Detention/ exclusion
Attempting to access the school network/ Learning Platform by using another pupil's account							
Attempting to access the school network/ Learning Platform by using the account of a member of staff							
Sending an email, text or instant message that is regarded as offensive, harassment or a bullying nature							
Unauthorised downloading or uploading of files							
Unauthorised use of a mobile phone/digital camera/other handheld device							
Unauthorised use of social networking/ instant messaging/personal email							
Accidentally accessing offensive or pornographic material							
Deliberately accessing or trying to access offensive or pornographic material							
Other….							

Action taken by ICT Technician: