E-SAFETY POLICY

E-SAFETY Policy - Document Status			
Date of Policy Creation	May 2017	**Named Responsibility for E-SAFETY**	Linzi Garner
Date of Policy Adoption by Governing Body	July 2017	**Review Date**	April 2018

‘Love, Laugh, Learn’

Responsibility, Respect, Resourcefulness, Reciprocity (teamwork), Resilience

Rationale

This policy outlines the school’s practice and procedures relating to the delivery of E-Safety. ICT in the 21st century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Wrockwardine Wood Infant School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for Wrockwardine Wood Infant. The internet provides an amazing opportunity for learning, exploration, entertainment and communication but there are risks associated with it. There are potential threats such as bullying or unwanted contact, many of which are regularly reported in the media and there are some things you would not like your child to see. We would not want you to stop your child from using the Internet, but you need to understand the risks and how to minimise them. We discuss a variety of issues related to staying safe online in school.
Our e-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school’s e-Safety Lead is Miss Garner
- The e-Safety Governor is Mrs Melhuish
- The e-Safety Policy and its implementation shall be reviewed annually.

Aims

We aim that through the Computing curriculum our pupils will:

- Provide a relevant, challenging and enjoyable curriculum for Computing for all pupils.
- Meet the requirements of the national curriculum programmes of study for computing.
- Use computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.

- To equip pupils with the confidence and capability to use computing throughout their later life.
- To enhance learning in other areas of the curriculum using computing.
- To develop the understanding of how to use computing safely and responsibly.

The new national curriculum for computing aims to ensure that all pupils

- Are responsible, competent, confident and creative users of information and communication technology. Explore issues related to living in a democratic society
- Become healthy and fulfilled individuals

Roles and Responsibilities

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the e-Safety Governor will include

- Regular meetings with the e-Safety Lead.
- Regular monitoring of e-Safety incident logs
- Reporting to the Governors.

Head teacher and Senior Leaders

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Lead.
- The Head Teacher/Senior Leaders are responsible for ensuring that the e-Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.
- The Head Teacher and Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Subject Leader

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-Safety Policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and report and log incidents to inform future e-safety developments.

The role of the Class Teacher:

- Teachers need to ensure that their timetables incorporate designated time for the teaching of e-safety each half term.
- Teachers need to be aware of the National curriculum aims and that they are being covered by the Entrust scheme of work and common sense media planning.
- Teachers need to ensure that the direct teaching of e-safety will follow a thematic approach through cross curricular work using the Medium Term plans for each year group
- Provide parents/carers with statements of their child's progress in their e-safety development in their annual report and through parent/teacher consultation.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content and filtering. This service is provided through Telford and Wrekin.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will have an e-safety lesson taught each half term using the common sense media scheme and take part in e-safety day each year.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- As part of the new computing (ICT) curriculum, all year groups have digital literacy units and PHSE that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying. This is taught through common sense media scheme of work.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

E-safety Content

The grid below shows specific E-Safety learning intentions for the EYFS:

ELG	EYFS
PSED Managing Feelings and Behaviour Understanding the World Technologies	Talks about their own and others behaviour and its consequences, and knows that some behaviour is unacceptable.(ELG) Works as part of a group/class, and understands and follows the rules. (ELG) Recognises that a range of technology is used in places such as home and schools. (ELG) Selects and uses technology for a particular purpose. (ELG)
Learning Objectives:	• Learn that staying safe online is similar to staying safe in the real world. • Be introduced to the basics of online searching. • Explore and comment on different types of websites with the teacher, which are pupils favourites and why? • Discuss how they use the computer/tablets at home and the difference between home and school use.
Resources	• Digi duck story: learn that staying safe online is similar to staying safe in the real world. • Chicken clicking story book • Smartie the penguin - eBook

	• Netsmartz - Router's birthday surprise • Netsmartz - delivery for Webster • Technology hunts

The children also will take part in safer internet day.

The grid below shows specific E-Safety learning intentions for Key stage 1:

	Year 1	Year 2
National Curriculum E-Safety and Digital Literacy	Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies	
Common Sense Media Scheme	• Going Places Safely Staying safe online • ABC Searching Simple search techniques • Keep it Private • Keep personal information private • My Creative Work	• Staying Safe Online Using sites suitable for age • Follow the Digital Trail Digital Footprints • Screen out the Mean • Introduction to cyberbullying • Using Keywords

	• Having ownership of what is yours • Sending Email • Communication in a digital world	• Efficient searching • Sites I like • Rating websites

The children also will take part in safer internet day.

Inclusion

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in our school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SENCO and individual teachers to ensure all children have equal access to ensure success in this subject.
Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information.

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in an e-Safety Log, which will be stored in the Head Teacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Lead.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Email

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Whole-class or group email addresses should be used in school rather than individual addresses.
- Access in school to external personal email accounts is not allowed.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a using Outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

- Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords, and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

Social networking Internet sites (such as Facebook and twitter) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact:
Use of social networking sites and newsgroups in the school is not allowed and will be blocked/filtered.

Pupils will be advised through e-safety lessons never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. (All staff are given guidelines in the Guide to Safer Working Practice.) The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-Safety Policy need to be recorded in the e-Safety reporting file that is kept in the Head Teacher's office. The details of the user, date and incident should be reported.
Incidents which may lead to child protection issues need to be passed on to the Designated Person immediately — it is their responsibility to decide on appropriate action not the class teacher's.
Incidents which are not child protection issues but may require Lead Teacher intervention (e.g. cyber bullying) should be reported to the Lead Teacher in the same day.
Allegations involving staff should be reported to the Head Teacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.
Evidence of incidents must be preserved and retained.
The curriculum will cover how pupils should report incidents.

Mobile Phones

Many mobile phones have access to the Internet and picture and video messaging, and such technologies present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying or inappropriate contact:

- All mobile phones will be kept in the nursery, school office or staff cloakroom/lockers throughout contact time with children this includes all staff, visitors, parent helpers, supply teachers and students.

- Parents are not allowed to use their mobile on the premises. If you find a parent doing this you should inform them of this and refer them to the Headteacher.

- Mobile phones will not be used when children are on the premises. However, if you have a personal emergency you are free to use the school phone or make a personal call from your mobile in the designated staff area of the setting (Nursery office, GP room, staff room or school office.)

- Staff will need to ensure that managers have up to date contact information and that staff make their families aware of emergency telephone numbers. THIS IS THE RESPONSIBILITY OF THE INDIVIDUAL STAFF MEMBER.

- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.

- Photographs and recordings can only be transferred to, and stored on a school computer to be printed.

- All telephone contact with parents will be done on the school/Nursery office phone.

- During group outings nominated staff will have access to the school mobile, and this will be used for emergency purposes only. On trips, staff mobiles are used for emergency only.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.
- Parents may take photos of their own children but should not upload pictures of their own child/children onto social networking sites from school (see guidance below).
  https://ico.org.uk/media/for-organisations/documents/1136/taking_photos.pdf

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email and telephone number.
- Staff and pupils' personal information will not be published.
- The Head Teacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified (permission sent at the start of each school year)
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil.
- Parents should not upload pictures of their own child/children onto social networking sites from school.
- The Governors may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them.

Protecting Personal Data

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

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaints about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet Safety will be displayed in all classrooms.
- E-safety lessons are taught each half term.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during computing and e-safety lessons, and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the school e-Safety Policy and its importance will be explained.

Parents:

- Parents' attention will be drawn to the school e-Safety Policy in newsletters and on the school website.

The following websites provide a range of resources, along with helpful guidance and information.

http://www.thinkuknow.co.uk/
http://www.childnet.com/
BBC Newsround Special programme on esafety
http://www.kidsmart.org.uk/
The UK Council for Child Internet Safety
https://www.nspcc.org.uk
https://ceop.police.uk/safety-centre/

Links to other policies and curriculum areas

We recognise the clear link between Computing and the following policies and staff are aware of the need to refer to these policies when appropriate.

Anti-bullying Policy

Acceptable use Policy
Child Protection Policy
Mobile Phone Policy
Computing Policy
Staff code of conduct
Photograph Policy

Appendices to this policy:
Appendix 1: Incident logs
Appendix 2: Responsible Use of the Internet (pupil)
Appendix 3: Acceptable ICT Use Agreement/ Responsible use of the internet (staff)
Appendix 4: permission for photographs to be taken
Appendix 5: Guide to safer working practice
Appendix 6: Social Networking in schools
Appendix 7: E-safety incident log

Appendix 2: Responsible Use of the Internet (pupil)

Wrockwardine Wood Infant School and Nursery

Responsible Computer Use: Pupils

These rules help us to be fair to others and keep everyone safe. School computers are for school work only.

- I will ask my teacher if I am not sure what is allowed.

- I will use only my own network login and secret password unless my teacher has given out a class login.
- I will only send messages to people I know, or people my teacher allows.
- The messages I send will be polite and sensible.
- From time to time I may see things which are unpleasant or that I know are wrong. If I see anything like this I will tell a member of staff as soon as possible.
- I understand that I must never give out my home address or phone number, or arrange to meet someone. I will tell a teacher if someone wants to meet me.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or the school computers.

The school may exercise its right to monitor the use of all the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is taking place, or the system is used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Monitoring is triggered when a violation of this policy is registered on the system.

Signed ……... *Date* _____

Appendix 3: Acceptable ICT Use Agreement/Responsible use (staff)

Acceptable Use Policy: Staff

The computer system is owned by the school. This Acceptable Use statement helps to protect students, staff and the school by clearly stating what use of the ICT resources is acceptable and what is not. If any further clarification is required please contact the Head of the school or the ICT for Learning department at the Local Authority.

- School computer and Internet use must be for educational purposes. Any doubt as to what constitutes educational use should be referred to the Head of the school.
- Network access must be made with the user's authorised account and password, which *must not* be given to any other person. When temporarily leaving a workstation it should be locked. (Ctrl-Alt-Del K) to prevent unauthorised access.
- Any messages should be written responsibly and politely. Abuse of any kind is forbidden.
- Users are responsible for any messages they send and for contacts made.
- Any unpleasant or inappropriate content should be reported to ICT services or the appropriate person in your school.
- Caution should be exercised before giving out any personal details, or information about the school, over the network.
- Anonymous messages and chain letters are not permitted.
- Not all resources on the Internet are free. Users must be aware of copyright and intellectual property rights before distributing content or resources.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT security systems must be respected; they are there for the benefit of all users. Any attempt to bypass security systems is a serious offence.

  The school may exercise its right to monitor the use of all the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of

Appendix 4: permission for photographs to be taken

<table>
<tr><td colspan="2">Wrockwardine Wood Infant School and Nursery
Responsible Internet Use & Parent Consent Form for Use of Pupil Images</td></tr>
<tr><td colspan="2">Parent’s Consent for Internet Access
I have read and understood the school rules for responsible Internet use contained within the School Prospectus pack and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.</td></tr>
<tr><td>Signed:</td><td>Date:</td></tr>
<tr><td colspan="2">Please print name:</td></tr>
<tr><td colspan="2">Parent’s Consent for Web Publication of Work and Photographs and Photographs in Printed Publications and Other Media as Part of the Promotional Activities of the School, eg DVD’s of celebrations
I consent to photographs and digital images of my child appearing in Wrockwardine Wood and Nursery printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the school.</td></tr>
<tr><td>Signed:</td><td>Date:</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Child’s Name</td></tr>
</table>

Appendix 5: Guide to safer working practice

Telford & Wrekin Safeguarding Children Board (SCB)

December 2014

Raising Awareness: Latest advice on the Safer use of Information Communication Technology (ICT) systems at home and in the workplace.

Introduction

You will be aware from the national media, that there have been a number of high profile cases regarding abuse of the Internet, mobile phones, e mail, social network sites such as Facebook and Twitter This can lead to Child Protection discussions and raises the issue of taking advice in terms of personal protection in the safer use of ICT.

At a local level this has been found to be no different, where there has been an increased caseload of allegations against individuals, especially those that work with children in their occupational status, some through sheer naivety. The situations that people find themselves in can be distressing, but this may have been averted at an earlier stage with some common sense guidance and tips for the protection of all computer users. Even if your work may not be with children this advice is useful to note.

Overview-The Safeguarding Children Board (SCB)

The Safeguarding Children Board is a multi agency arrangement which replaced the Area Child Protection Committee's. The Board members represent their organisations at the most senior level and were established under HM Government's "Working Together to Safeguard Children".

The SCB has a number of senior ranking individuals as members in organisations across multi agency disciplines. Every Local Authority has to have a SCB in place. Officers of the board are charged with investigating allegations against all staff where there may be child protection concerns, these Officers are known as the Local Authority Designated Officers (LADO).

Although the SCB is specifically aimed at children and their welfare, the SCB feels it has a duty to provide guidance to all ICT users, This is especially true in regard to self protection in the ever changing world of technology, in or out of work, whether child or adult..

Action

After discussions about recent cases at a local level with the School Community, Telford & Wrekin Council Officers, Union Officials and Officers from the Safeguarding Children Board, some guidance was produced specifically for schools back in 2007 and 2011.This new guidance is for general use but does reflect those that may work with children and young people but it is felt that everyone should be aware of this advice.

Safer use of Social Networking-Internet-Phones-Email

Using New Technology - Hints and Tips for staff working with children and young people

Read this, it might be helpful even if you don't …

Social Networking hints and tips

Social networking sites are excellent ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal, they are often set for all to see! Be web savvy!

- Social networking sites, such as the currently most popular "Facebook", **have a range of privacy settings**. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details,

photographs etc., can only be seen by your invited friends **(please see the attached example on setting to privacy, also the attached Facebook Checklist).** Please note that other providers have similar settings so that access is restricted.

- Have a neutral picture of yourself as your profile image. Don't post embarrassing material. Be careful what you post! Increasingly companies and organisations "trawl" open Facebook profiles before they interview or appoint!
- You do not need to accept friendship requests. Reject or ignore them unless you know the person or want to accept them. Be prepared to be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about **their** privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile. Check it out!
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school/youth project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Never knowingly give permission for students to take your photograph with their own mobile phone
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.

- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the "WayBackMachine".
- Think about your internet use, adults are just as likely as children to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password.
- In the workplace and in all Telford schools, ICT systems are monitored. If you are surfing the Internet and visit inappropriate sites it will be recorded. If you visit inappropriate sites, this could lead, in the worst cases, to a criminal prosecution and disciplinary action. For avoidance of doubt please acquaint yourself with your work Corporate Information Security Policy (CISP) and Social Media Policy. Also if sites are visited inadvertently make your Senior Management Team aware and seek advice from your ICT Team.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any word found in a dictionary.
- Be careful when form filling online…., do you know who the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.
- Never verify banking details online.
- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.
- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.
- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact), do not give out any personal information.

- Popup adverts are often a nuisance. Close them carefully as a ‘close’ button will often lead you to more advertising as the ‘X’ might be a graphic.
- If you get an email or popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.
- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing ‘adult content’ on your computer, the stored cookies may mean you get ‘adult pop-ups and adverts’.
- Use legal sites for downloading music, films etc., such as iTunes.
- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.
- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as ‘net play’. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.
- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be ‘throttled’ - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.
- When you log-into a web site, unless your computer is exclusive to you, don’t tick boxes that say ‘remember me’.
- Don’t leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Don’t give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.

Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into ‘pages’ in a document, Learning Platform, or interactive whiteboard resource etc.
- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.
- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.
- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.
- Watch YouTube (or any) videos before you use them in the classroom.
- If you use a YouTube (or any) videos, find out how to embed it using the ‘Source’ rather than a page link, as that exposes pupils to other content. You will also need to uncheck the box which allows the embedded video to suggest related videos.
- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.
- If you want to use a clip download it (if legal & copyright allows). Otherwise it might not be there next time you look for it.
- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.
- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership’s permission, and ensure it is on an encrypted device.
- Remember that if you leave a computer running and leave the room it can be tampered with by students and may leave you open to exploitation. Wherever possible, good practice would be to lock the computer by pressing Ctl-Alt-Del and press K for the duration of your absence

- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.

You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the NEN, Learning Platform or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.

Email hints and tips

- Keep all your work and private transactions separate. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.
- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.
- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.
- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.
- Webmail is useful but insecure, and your email address is easily passed on.
- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.
- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.
- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.
- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don’t give out your mobile number or home number to students, pupils or service users, unless there are exceptional reasons to do so *(see below).*
- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.
- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from ‘stranger’ devices within range.
- Be very careful what you store on your mobile phone, if it is taken by anyone they may get information which could be embarrassing in a number of ways

Are there any circumstances where it may be considered that legitimate use of ICT interaction with young people and service users is acceptable, through my work and in exceptional circumstances outside of work?

It is recognised that there may be exceptional circumstances where it is acceptable within or outside of work to have legitimate contact via ICT methods. Within the school network this is closely monitored but all staff should, if they have to, liaise via work based equipment, this shows transparency. However, the balance, proportion and culture has to be right and no one would wish a child or service user to come to harm because of bureaucracy and a lack of common sense in decision making and not “doing the right thing”.

It may also be considered that other exceptional circumstances could be considered appropriate, these include;

- Outdoor Trips, especially outdoor pursuits and those abroad. It would be entirely appropriate and for the duration of such activities for children to be safe and in contact with those leading them

- Children or service users who are classed as “gone missing” should always be reported through to the Police without delay. However, on Police advice and only on instruction by them on a case by case basis, there may be exceptional circumstances where staff could be judged to be more appropriate to make personal contact, this would be exceptionally rare. For example this could be considered where the Police feel their presence may inflame a situation.

- Youth Offending Service, Health, Sexual Exploitation, Therapeutic and Social Care Teams sometimes manage appointments by text messaging, where often this is the most appropriate way that young offenders, patients and service users engage and manage to keep appointments

- Professional judgement, where in the absence of the need of direct Police intervention, immediate action is necessary for the immediate safety or concern of any child, service user or those people around them.

Keeping legitimate contact real in the ICT world

Advice for all is to be accountable for your actions, including some useful tips to follow;

- Where possible use work based ICT Systems and processes
- If personal ICT Systems are used clearly account for that use
- Clearly action your rationale and reason as to "why"
- Document your actions and show transparency
- Be mindful/sensitive of "tone and content"
- Be aware of professional boundaries and recognising early indications of imbalances in that relationship
- In what context did the exceptional; circumstances occur, and
- If Communication is to be made within your organisation, then make that clear to your line manager for endorsement at the outset

Facebook-Briefing note on setting your status to privacy

This briefing note is not aimed at the use of Facebook in school or the workplace, ***but has implications for e safety and privacy for all Facebook users*** – adults and young people.

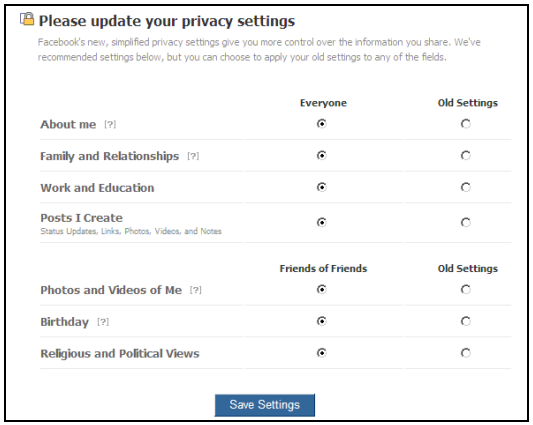
Facebook are currently directing all users to review their privacy settings through an on screen message window.

Why is this a concern?

- The process may lead Facebook users to widen access to their personal information from **friends only** to **everyone** without realising it.
- We are aware many pupils use Facebook, including young people at Primary schools. The age restriction for Facebook is 13 but many young people use Facebook with parental permission so we would not recommend asking Facebook to routinely remove all underage profiles unless there are issues such as cyberbullying or inappropriate contact or posting.

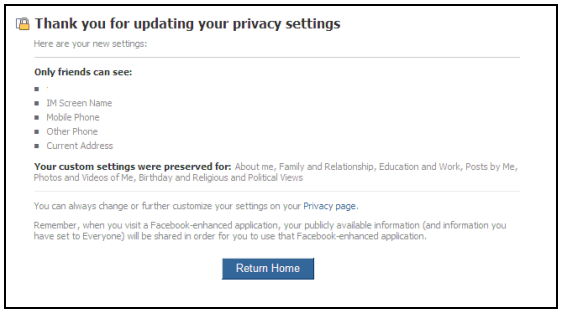
What does the Privacy settings review look like?

If you say **continue to next step** you get the screen below, notice it has suggested opening the profile up to everyone – the temptation is to just select **save settings** and as a result open up your privacy to everyone.



We strongly recommend users to:

- Keep old settings
- Only share with Friends
- Do not share with everyone



To check your privacy settings

- Log into Facebook
- Selects settings from the top bar (right hand side)
- then privacy settings
- profile information

If you have concerns – reporting issues to Facebook

Facebook will only follow up concerns if their terms and conditions have been breached

- Email from a school email address only to abuse@facebook.com
- Include the URL of the profile you are reporting – the name of the person is not sufficient
- State why the profile/page breaches terms and conditions (http://www.facebook.com/terms.php) e.g. pupil is under age 13, the profile is an imposter etc.
- Put your contact information, including your job title etc.

Appendix 6: Social Networking in schools

It is widely acknowledged that social networking can play a valuable part in education, but equally misuse of these applications can cause great damage to the moral and well being of students, parents and staff.
Social networking applications include, but are not limited to:

- Blogs
- Online discussion forums
- Collaborative spaces (for example *Facebook*)
- Media sharing sites (for example *You Tube*)
- Micro blogging applications (for example *Twitter*)

All members of a school community have an obligation to use social networking in a responsible way and should bear in mind that information shared through these applications are still subject to copyright, data protection, freedom of information legislation, and other legislation including (but not exclusively) the **Protection from Harassment Act 1997**, **Malicious Communications Act 1998**, **Criminal Justice and Public Order Act 1994** and the **Communications Act 2003.**
All Telford & Wrekin schools endorse the rights of freedom of expression, however the use of social networks must pay due consideration to the rights of others. It is recommended any use of social media be in accordance with the following **Code of Conduct**.

♣ **Proposed T&W Schools Social Networking Code of Conduct**

Social Networking applications must not be used to publish any comment which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes material of an illegal, sexual or offensive nature that may bring a school into disrepute.
Social Networking applications must not be used for the promotion of personal financial interest, commercial ventures or personal campaigns.
Social Networking applications must not be used in an abusive or hateful manner.
Social Networking applications must not be used for actions that would put school representatives in breach of school policies.
Social Networking applications must not breach the school's misconduct, equal opportunities or bullying and harassment policies.
Social Networking applications must not make reference to any pupil, parent, member of staff or school activity / event unless prior permission has been obtained and agreed with the head teacher.

School staff should be aware that if out-of-work activity reported on social networking applications causes potential embarrassment to the school or detrimentally affects the school, then the school is entitled to take disciplinary action.[i]

The following flow chart illustrates the course of action to be taken upon a breach of the Code of Conduct:

[1] NB. **This should form part of the IT policy that all staff sign up to; and include guidance on interaction with pupils**

Suggested Timeline

Appendix 7: E-Safety Incident Log

Wrockwardine Wood Infant School and Nursery e-Safety Incident Log

Details of ALL e-Safety incidents should be reported to a DSL who should record the details below. This incident log will be monitored termly by the Headteacher, Member of SLT, Safeguarding Team, or Chair of Governors.

Date and Time	Name of pupil or member of staff	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons