E-SAFETY POLICY

St Egwin's C.E Middle School

Approved by:	N Pullan	**Date:**	12/6/18
Last reviewed on:	1/1/2020		
Next review due by:	1/1/2021		

Rationale

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.

The Internet Policy is available on the school website and parents/guardians have to sign to say they have read it.

We have introduced the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.
The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

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

- Responsible ICT use by all staff and pupils; 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 Worcester LA Network including the effective management of 'Policy Central'.
- National Education Network standards and specifications.

The e-Safety Policy relates to the school's safeguarding policies and practices as well as to other policies including those for ICT, Anti-Bullying and Safeguarding.

- The school's e-Safety Coordinator is A Higgins.
- Our e-Safety Policy has been written by the school, building on the St. Egwin's e-Safety practice and government/local authority guidance. It has been agreed by staff and approved by Governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by N Pullan and A Higgins

Roles and Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors
Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT and E-Safety Coordinators
- Regular monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors and/or committee(s) meetings.

Headteacher & Senior Leadership Team (SLT)
The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety Coordinator
The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school

ICT Coordinator
The ICT Coordinator is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

Teaching & Support Staff
In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy.

- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Education and Training
E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Computing and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy

- **Parents/carers** will be required to read through and sign alongside their child's signature in their child's planner, helping to ensure their children understand the rules
- **Staff and regular visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.
- **All users will accept the AUP each time they log into the school IT system.**

Copyright

- Pupils to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations - staff to monitor this.
- Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / pupils should open the selected image and go to its website to check for copyright.

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or safeguarding.

Communication
E-safety rules will be posted in all class rooms and the ICT suite and discussed with the pupils at the start of each term. Pupils will be informed that network and Internet use will be monitored.
Email

- Digital communications with pupils via e-mail should be on a professional level and only carried out using official school emails.
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems) or Outlook;
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.

- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

Mobile Phones

- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.
- When on school trips the school will provide staff with mobile phones for communicating with school.
- All mobile phones from Key Stage 2 pupils are signed into the office at 8.20 in the morning. Key Stage 3 pupils with access to a locker must keep their mobile phone in their locker during school hours. Any pupil in Key Stage 3 without a locker must also sign their mobile phone into the office at 8.20am.

Social Networking Sites

Pupils will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Pupils/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Pupils will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list can be obtained from the school office.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of pupils.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems

Pupils

- Should only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten. The ICT co-ordinator and ICT technician are able to access the network to allow students to change passwords.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or ICT co-ordinator.
- Pupils should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring & Reporting

All use of the school's Internet access monitored. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Key Stage Co-ordinators, members of the Safeguarding Team or members of the Senior Leadership Team depending on the severity of the incident.

- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Headteacher).

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Assessing risks

• 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
Worcestershire LEA can accept liability for the material accessed, or any consequences of Internet access.
• The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

• Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team.
• Any complaint about staff misuse must be referred to the Headteacher.
• Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
• Pupils and parents will be informed of the complaints procedure.