Tidbury Green School
Dickens Heath Road
Tidbury Green
Solihull
B90 1QW

Policy Name

E-Safety

Date of Review

Spring Term 2024

Next Review Date

Spring Term 2026

Agreed by Governors

……

Date

……

Policy:	E-Safety
People Authorised to make changes to this policy:	• Mrs R Fitter • Mr T Griffiths • Miss J Styler
Committee responsible for approving policy:	Full Governing Body

Questions for the reviewer of this policy:	
Does this policy comply with statutory requirements and is relevant legislation and guidance referenced in the policy?	**Yes**
Does the policy reflect current evidence-based good practice?	**Yes**
Is the policy consistent with the vision and ethos of the school?	**Yes**
Does the policy reflect current practice in the school?	**Yes**

After policy review:	
Changes made:	No major amendments needed.
Expected impact of updated policy:	
Updated policy sent to governors:	Feb 2024
Updated policy sent to staff:	Feb 2024
Updated policy put on website:	Feb 2024

Development, monitoring, and review of this policy

This e-safety policy has been developed by a working group made up of:

- *Headteacher:* ***Mrs R Fitter***

  Assistant Headteacher: ***Mr T Griffiths***
- *Computing Lead:* ***Miss J Styler***
- *Governors*

It has been written by the Computing co-ordinator after conversations with the DSL. Before being finalised, it has been shared and edited with staff, including teachers, support staff and technical staff and has been shared and discussed with governors. It is available to parents to view on the school website. Consultation with the whole school community has taken place through a range of formal and informal meetings.

- Our e-Safety Policy has been written by the school, building on the Solihull LA e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually in order to keep up to date with technological advances.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities 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 Governors has the role of overseeing safeguarding, which encompasses e-safety.

The role of this governor will include:

- meetings with the E-safety co-ordinator
- monitoring of e-safety incident logs
- monitoring of filtering/change control logs
- reporting to relevant Governors
- evaluating the effectiveness of E-Safety INSET training.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to DSLs and the Computing Lead.

- The Headteacher and Senior Leaders are responsible for ensuring that DSLs, the Computing Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and 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 support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will also evaluate the effectiveness of E-Safety INSET training (in school and external).
- If the E-Safety policy is misused, appropriate sanctions and actions will be taken by the Headteacher.

E-safety Co-ordinators

DSLs receive reports of e-safety incidents through MyConcern and these inform future e-safety developments. The safeguarding governor is also kept aware of incidents and able to discuss current issues, review incident logs and filtering/change control logs when needed.

Along with DSLs, the Computing Lead:

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and 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 technical staff
- Reports regularly to Senior Leadership Team
- Provides parents/carers with updates regarding social media and e-safety issues

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher for investigation
- All digital communications with pupils/ parents/carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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
- They remain compliant with the Data Protection Law

Pupils

Pupils:

- Are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Have a good understanding of 'Apps', 'Filters' and Photo Editing
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- 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 covers their actions out of school, if related to their membership of the school
- The self-esteem, well-being and mental health of our pupils will be a consideration with any of our school policies
- Are made aware that any issues regarding cyber bullying will be dealt with accordingly in line with our anti-bullying policy.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, letters, website and e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events (see Mobile Phone Policy)
- Their children's personal devices in the school (where this is allowed)

Parents/Carers **must** hand their mobile phones and other technological equipment into the office before entering the main part of the school.

Why is internet use important?

- As our students mature, they learn how to recognise difficult situations in many areas. We will help them understand and be safe in the online world.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who are encouraged to show a responsible, respectful and mature approach to its use.
- 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.
- Pupils use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does internet usage benefit education?

- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.
- technology provides access to experts in many fields for pupils and staff;
- access to world-wide educational resources including museums and art galleries;

How can internet use enhance learning?

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The internet, when used responsibly, can widen a child's area of knowledge and provide new opportunities to extend their learning.

How will pupils learn how to evaluate internet content?

- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Following our Purple Mash scheme of learning, pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- In line with the curriculum, each year group has a designated 'Online Safety' unit; this is where they learn to both utilise and evaluate the internet (for example, examining a social media account to assess if the data on it could be compromising or inappropriate).

- As well as the internet units covered in every year group of our Computing curriculum, we also explore important themes during Safer Internet Day.
- Pupils are taught how to recognise safe/trustworthy websites and the appropriate settings to take.

How will information systems security be maintained?

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Staff have the use of secure 'Remote Access' from home when required.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- The Computing Lead / network manager will review system capacity regularly.
- We employ an IT Technician to maintain our school information system who works alongside the local authority.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts. On joining the school, each pupil is given their own Solihull e-mail address (@tidbury-green.solihull.sch.uk)
- Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils have been taught 'See it, minimise it, report it', so that offensive e-mails can be examined and acted upon.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils may only contact members of staff via email regarding school business, not socially.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils in all year groups have an 'e-mail' unit as part of their Computing curriculum, where they learn to send and receive e-mails safely.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully to avoid spam harvesting.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can a pupil's images or work be published?

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Parents sign consent forms before images of their children are published on the website or elsewhere.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

How will social networking and personal publishing be managed?

- The schools will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messenger and e-mail addresses, full names of friends, specific interests and clubs etc.
- Class blogs or wikis are run from the school website or securely through Purple Mash. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged through Computing lessons to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Students and their families are advised not to post pictures revealing personal information such as their school.

How will filtering be managed?

- If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Lead.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP.
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by engineers.
- Before using a website, staff should check if it is safe to use and is appropriate to the age group.
- Senior staff should review which material is blocked and document decisions on what is blocked or allowed and why.
- Be aware of new technologies that may get around the filtering such as VPN.
- If staff/pupils search for something deemed inappropriate, a blocked message should show on the screen and a report of this is sent to the Headteacher with the name, time, date and IP address. This should be dealt with appropriately.
- Filtering, however, should not lead to an unreasonable amount of restrictions as we still need to teach online safety and safeguarding.
- Staff can monitor usage within class by supervising/observing what children are accessing.
- Continue to use filtering services provided by the local authority that has been designed for schools.
- As our filtering system is managed by Solihull, senior leaders liaise with their IT department.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

How will internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised internet access.

How will risks be assessed?

- The school should audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?

- Complaints of internet misuse will be dealt with by a senior member of staff/DSL.
- Any complaint about staff misuse must be referred to the head teacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety policy in newsletters, the school brochure, on the school website and social media pages.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This could include suggestions for safe home internet use alongside parent workshops.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to relevant organisations.

How will Child Protection be ensured?

- Children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
- The school has a responsibility to educate pupils and teach them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, particularly social networking sites. Parents will be included as much as possible in this process so that they can ensure that any access the pupils have to computers and the internet at home is safe.
- Appropriate photographs are taken of children to capture a curriculum activity or a celebration of school life using school equipment but permission will be sought from parents beforehand. Staff will not use their personal mobile phone, camera (still or moving images) or other devices to take, edit or store images of pupils from this school.

- Any concerns will be immediately reported to a DSL.
- Staff will not communicate with pupils through private email accounts, work email accounts, or social networking sites. Staff will be circumspect in their use of social networking sites and will not discuss school business or school issues on their personal social networking site. The school believes it is far safer for staff not to accept either school children or ex-pupils as 'friends'. Great care will be taken if staff make an exception to this guidance and will account to the Head teacher for their decision e.g. the young person is also a family member.
- For further information about Child Protection, please refer to the Child Protection Policy.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	**Staff & other adults**				**Students/Pupils**			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones/cameras				X				X
Use of other mobile devices (as examples tablets, gaming devices)		X						X
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails	X					X		
Use of messaging apps		X				X		
Use of social media		X				X		

Use of blogs		X				X		

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, school Facebook or Twitter pages etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.