TALBOT PRIMARY SCHOOL

Online Safety Policy - DRAFT

Academic Year 2022-23

Head teacher – Kate Curtis

To be Ratified by Governors

HAMWIC
EDUCATION
TRUST

Overview of policy

Talbot Primary School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. The online policy is for the academic year of 2018/19. The subject of Computing 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 Talbot Primary School we need to build in the safe and responsible use of digital technologies, in order to arm our young people with the skills to access life-long learning and employment. Online safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe digital environment for Talbot Primary School. As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

Headteacher/ Senior Leaders

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by the governors. The following has been agreed in line with the Online safety Policy.

- The school’s Online safety Co-ordinator is Mr C Brown

- The Online Safety Policy and its implementation shall be reviewed annually.

- Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. Regular meetings with the Online Co-ordinator/Officer.

- Regular monitoring of Online safety incident logs.

- Reporting to the Headteacher and Senior Leaders of any incidents which are involving Online safety.

- The Headteacher is responsible for ensuring the safety (including Online safety) of members of the school community, though the day-to-day responsibility for Online safety will be delegated to the Online safety co-ordinator.

- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher/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 Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and Assistant Heads should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incidents taking place

- The Hamwic Trust will provide updated training and advice for staff.

- Liaises with school Computing technical staff.

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 filtering.

- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation (during ICT lessons).

- As part of the new Computing curriculum, all year groups have digital literacy objectives 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.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Through computing, 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 this 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 our SENCO and individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line 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:

Staff

- All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any digital school 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 Headteacher, by recording the incident in Online safety log, which will be stored in the Online Safety Co-ordinator’s office.

The Online Safety log will be reviewed yearly by the Online Safety Co-ordinator and the DSL.

Internet

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

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of Online Safety.

- Pupils may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Whole class or group e-mail addresses should be used in school rather than individual addresses.

- Children are not to access in school to personal e-mail accounts is not allowed.

- E-mail 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

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 Twitter, Facebook) 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 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. 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 Online safety policy need to be recorded on My Concern by a member of staff.
- 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 one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers. 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 (e.g. Ceop button, trusted adult, Childline) Mobile Phones Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they

present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

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, e-mail and telephone number.

- Staff and pupils' personal information will not be published.

- One of the Headteachers 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.

- 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 only upload pictures of their own child/children onto social networking sites.

- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School IT 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.

- Online Safety will be discussed with our Computing support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data 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.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to one of the Headteachers.

- 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

- Rules for Internet access will be posted in all networked rooms.

- Pupils will be informed that Internet use will be monitored.

- Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons. Staff:

Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School's Online Safety Policy in newsletters and on the school Website.

Camera Mobile Phones

- Camera mobile phones are now the norm and a built in digital camera enables users to take high resolution pictures. These can be sent instantly to other mobile phone users or email addresses. They can also be posted on the internet or in chat rooms. There is a potential for camera mobile phones to be misused in schools. They can become an instrument of bullying or harassment directed against pupils or/and teachers.

Smartphones

- The misuse of social media sites, messaging services is an ongoing problem. Many of these sites have a recommended age which is above that of primary school pupils. This is because many children are not mature enough to use these sites appropriately, putting themselves or others at risk or using them as a tool to be unkind to their peers. Whilst we can only advise parents of how to help their children engage with their phones and the internet outside of school hours, we do have a duty of care to our pupils and cannot allow children to have access to smartphones during school time to ensure we can keep everyone safe.

Mobile Phone Policy for pupils in school

- While we fully acknowledge a parent's right to allow their child to bring a mobile phone to school if they walk to and from school without adult supervision, Talbot Primary School discourages pupils bringing mobile phones to school due to the potential issues raised above.
- When a child needs to bring a phone into school, a permission slip (Appendix 1) must be signed by the parent and the phone must be left in the school office at the start of the day and collected at the end of the day. Phones should be clearly marked so that each pupil knows their own phone.
- Parents are advised that Talbot Primary School accepts no liability for the loss or damage to mobile phones which are brought into school or school grounds.

- Where a pupil is found by a member of staff to be using a mobile phone, the phone will be confiscated from the pupil, handed to a member of the office team who will record the name of the pupil and attach it to the phone. The mobile phone will be stored by the school office. The pupil may collect the phone at the end of the school day. A letter will be sent home to parents requesting that a permission slip be returned the next day. If this practice continues more than three times, then the school will confiscate the phone until an appropriate adult collects the phone from a senior teacher.

- If a member of staff suspects that a pupil has a mobile phone in school then they will conduct a search, in line with government guidance. Should a device be found, this will be stored in the school office and the parents informed.

- If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken according to our behaviour policy.

- If images of other pupils or teacher have been taken, the phone will not be returned to the pupil until the images have been removed by the pupil in the presence of a senior teacher. (Please see more guidance on sexting in our child protection policy).

- Should a pupil be found to be using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.

- We ask that parents should talk to their children about the appropriate use of text messages as they can often be used to bully pupils.

- Should parents need to contact pupils or vice versa during the school day, this should be done via the usual school procedure of contacting the school office via phone or email.

Staff policy

- Staff use of mobile phones during their working day should be:
- ⍰ outside of their directed time with pupils
- ⍰ discreet and appropriate eg: not in the presence of pupils
- Mobile phones should be switched off and left in a safe place during lesson times. The school cannot take responsibility for items that are lost or stolen. Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, they should use the school telephone in the office.
- Staff should never send to, or accept from, colleagues, parents or pupils, texts or images that could be viewed as inappropriate.