Talbot Primary School

Computing and Online Safety Policy

Reviewed/Revised: September 2023

Next review: September 2026

Office use:

Statutory	-
Web	✓
Staff Notices	✓

Rationale

At Talbot, we inspire children to learn computing by offering them quality, first-hand experiences. We understand that an overwhelming majority of pupils love digital technology and want to embrace it; therefore, we celebrate computing and actively demonstrate that we have a shared understanding of the benefits it can offer.

Computing lessons are discrete in order to teach the key skills, these skills are then used to support other subjects. **Talbot's approach is based around three areas of learning; computer science, information technology and digital literacy**. These core concepts are revisited every academic year, deepening pupils' knowledge and understanding in a spiral curriculum. Key vocabulary is introduced carefully to the children, at the start of each topic, and it is used regularly in context to embed understanding.

The curriculum is based on the teaching sequence outlined in the National Curriculum. There is a strong focus on skills, as this enables pupils to become independent, life-long learners in a changing world. The curriculum is then made distinct by basing it on the Purple Mash computing scheme of work; Purple Mash ensures full coverage, support and progression within year groups and over time. Teachers adapt their teaching to fit the needs of their cohort. The teaching of computing also extends far beyond the discrete computing lessons. Key messages are delivered in other areas of the curriculum such as PSHE, class assemblies and whole school assemblies; there are also themed weeks. Online safety is an essential part of our teaching and learning, as it supports school's overall safeguarding culture and processes. The 'Digital Ambassador' programme is effective; trained pupils promote key online safety messages to their peers in school.

Ongoing feedback and mini assessments underpin the teaching and learning cycle in computing; this formative approach enables teachers to intervene immediately. Year groups assess pupils against the body of knowledge they are expected to have learnt each term. By the time children leave Talbot, they are digitally literate, intelligent and safe users of technology, using it to enrich and support their lives. They are able to express themselves appropriately, develop their ideas and entertain themselves. This prepares them for a digital world and a digital workplace.

Aims

Talbot Primary School is an inclusive, friendly community school, striving for excellence and enjoyment. Children will leave our school as kind, confident and resilient citizens with a passion for learning. The teaching and learning of computing helps realise this ambition.

The policy for computing supports our three core values of **"Courage, Truth and Loyalty,**" which form the school motto. The policy also helps deliver the four areas outlined in our curriculum visual: be ready and able, get creative and get thinking, aim high, and invest in "you."

The delivery and impact of the whole school curriculum is described in the 20-point School Curriculum Statement, providing consistency in approach. This policy focuses on the role of the Subject Leader, and it describes how the approach to computing is adapted to make it distinctive to Talbot Primary School.

The school aims to:

- provide a relevant, challenging and enjoyable curriculum for all pupils.
- meet the requirements of the national curriculum programmes of study for computing at Key Stage 1 and Key Stage 2 as specified in our 3-11 curriculum, including Nursery and Reception
- equip pupils with the confidence and skills to use digital tools and technologies throughout their lives.
- promote the enjoyment and benefits of computing.

- ensure the internet is used appropriately and safely, protecting the pupils from undesirable content through education and systems.
- ensure we have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- identify and support groups of pupils that are potentially at greater risk of harm online than others
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- enhance and enrich learning in other areas of the curriculum using computing.
- ensure children, parents, staff, governors and the wider community have increased access to information through computing.

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study (see below)

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see appendices)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Headteacher will lead the computing working party (HT, Computing subject lead and internet providers) to regularly review and ensure the following:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring the school also implements a robust filtering and monitoring system which encompasses the Internet Watch Foundation URL and image hash list, as well as the Home Office Terrorism Block List. As a result the school meets its online safety commitments as part of our Prevent Duty.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily/weekly/fortnightly/monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting senior leaders to ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with leaders and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

<u>All staff and volunteers</u>

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (see appendices)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by systematically reviewing practice and actions
- Following the correct procedures by discussing requests with the DSL or Deputy if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

<u>Parents and carers</u>

Parents and carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendices)

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International

- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum as specified in the national curriculum. Schools also have to teach Relationships education and health education in primary schools (see RSE policy)

In **Key Stage 1 (KS1)**, pupils will be taught to:

- 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

Pupils in **Key Stage 2 (KS2),** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.
Teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND (see pedagogy section)

Educating parents and carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website, curriculum and headteacher newsletters. The school will let them know what systems the school uses to filter and monitor online use and what their children are being asked to do online, including the sites they will be asked to access. This policy will also be available for parents and carers to view on the school website. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim, e.g. 'Zip it, Block it, Flag it.'

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This is built into our personal, social, health and economic (PSHE) education learning, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see training section for more detail).
The school also sends information/leaflets on cyber-bullying to parents and carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set in our behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or most senior member of staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents and carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Talbot Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. Talbot Primary School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable use of the internet in school

All pupils, parents and carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.
More information is set out in the acceptable use agreements.

Pupils using mobile devices in school

Pupils may not bring mobile devices into school. Parents and Carers should contact the school to discuss any requests. All phones will be stored in the school office at the start of the school day and returned at the end of the school day.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Reporting any issues with anti-virus and anti-spyware software to our network providers, i.e. Primary ICT

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the appendices and ensure they adhere to practice as specified in the Guidance for Safer Working Practices document

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Training will also help staff to develop:
    - better awareness to assist in spotting the signs and symptoms of online abuse
    - the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
    - the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL, Deputy DSL and Child Protection Officers, will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL and Deputy DSL log behaviour and safeguarding issues related to online safety on CPOMS. Reporting will ensure details are accurately recorded and associated actions, i.e. date, where the incident took place, description of the incident, action taken and the name of the staff member recording the incident. The Governing Board will be provided with an overview of incidents via the half-termly Headteacher report.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board if significant updates are required. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Pedagogy for computing

The Subject Leader for computing, ensures that the subject has a strong profile across school, and it is given the time and space it requires in the curriculum.

Organisation

Early Years

In Early Years, the children learn the fundamental building blocks for this subject. The teaching of computing in early years is integrated into the whole curriculum as a way to support children's learning and communication across all the different areas of learning. It is important in the foundation stage to give children a broad, play-based experience of computing in a range of contexts, including outdoor play. Computing is not just about the use of computers. Early years learning environments should feature scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to write or paint on the interactive whiteboard or program a toy. Recording devices can support children to develop their communication skills. This is particular useful with children who have English as an additional language. Different technological toys are provided in the areas of provision for children to access e.g. torches, cars, cameras, mobile phones. This supports and extends the skills children develop as they become familiar with simple equipment and techniques such as twisting or turning a knob. Devices are also used in order for children to record their own learning.

Key Stage 1 and 2

From Year 1 to Year 6, computing is taught once a week for 1-hour. Objectives are taught discretely, developing skills based learning and children are given the opportunity where possible to apply these skills in different areas of the curriculum.

Key Stage 1

By the end of key stage 1, pupils should be taught to:

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions
- write and test simple programs
- use logical reasoning to predict and computing the behaviour of simple programs
- organise, store, manipulate and retrieve data in a range of digital formats
- communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Key Stage 2

By the end of key stage 2, pupils should be taught to:

- design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs
- use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs
- understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration
- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely
- select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Key areas of learning

The computing curriculum puts a clearer emphasis on three areas of learning:

- **Computer science** - how computers work and how to write algorithms and solve problems to eventually create a computer program;
- **Information technology** - how data is represented and managed on computers;
- **Digital literacy** - how to understand digital information and interact with it safely and appropriately. This is in direct compliance with the key requirements of the DfE's Teaching Online Safety in schools programme and associated Education for a Connected World documents.

Long term planning

The Subject Leader is responsible for ensuring that the National Curriculum objectives for computing are taught thoroughly and systematically over seven years, ensuring vertical progression of the core knowledge and skills. Lessons are planned using the National Curriculum 2014 objectives, with the Purple Mash computing scheme of work tailored to effectively meet the needs of each cohort. Teachers also ensures that objectives have been organised and adapted to match the needs and context of pupils at Talbot Primary School.

Medium term planning

Class teachers are responsible for the teaching and learning of subjects in their year groups. They work collaboratively, supporting the robustness of learning and consistency across parallel classes. The computing scheme of work ensures progression, challenge and knowledge is taught to allow the effective development of skill. Subject leaders ensure standards remain high through monitoring, assessment review and pupil interviews.

Whole school teaching and learning approaches

Delivery and impact of learning in computing is fundamentally supported by the three whole-school, teaching and learning approaches, which underpin Talbot's unique teaching and learning philosophy. These are:

- Teaching through Metacognition, so pupils better understand the learning process
- Fostering a Growth Mindset approach to learning to develop learning characteristics
- Using Talk Matters strategies to ensure every child talks, in every lesson, thereby building and developing their mastery of subject specific language

Resources

The subject leader is responsible for ensuring that resources are adequate for delivering this subject successfully, including deep learning. Class teachers will make the subject leader aware of any deficiencies in the resources they need. The school acknowledges the need to continually maintain, update and develop its resources and to make progress towards consistent, compatible computer systems by investing in resources that will effectively deliver the requirements of the National Curriculum. Equipment is maintained to the meet agreed safety standards and teachers are required to report any faults as soon as they are noticed. Our computing network infrastructure includes:

- Interactive whiteboards in each classroom across the school
- A computing suite of 30 computers.
- A set of 30 Ipads in each phase, including Nursery and Reception.
- Wi-Fi internet access is available in all classrooms.
- Every class has an allocated slot one session per week for teaching computing as a discrete subject.

A list of computing software and hardware is maintained by the office staff, with old equipment removed from the inventory and disposed of safely. This is in compliance with GDPR protocols.

Assessment

Class teachers are responsible for the direct assessment of computing. The bedrock of sound assessment is formative techniques, which reveal pupils understanding and allow teachers to respond to needs immediately. Formative assessments also facilitate timely adaptations to the planning and delivery of computing. Year groups assess pupils against the body of knowledge and skills they are expected to have learnt, in alignment with the National Curriculum, each term. The data is collected and analysed using O-Track. Performance in lessons is the main way pupils are assessed.

- The children's work is saved on the school network and the school's Purple Mash account.
- Assessment will be carried out in line with the School Policy on Foundation Subjects.
- Progress is assessed using the key objectives and age related expectations for computing.
- Formative assessment methods are utilised to implement a best-fit judgement

Training

The subject leader is responsible for delivering CPD for computing. This is done through INSET, Staff Meetings, bespoke 1:1 training and signposting resources and opportunities. Teachers are given delegated time to study subjects and learn more deeply about them. The SLT support the Subject Leader.

Special Educational Needs and Disabilities

All pupils are expected to make good progress and gain from learning about computing. Teachers are aware of the differing needs of individuals in their class. Children who have identified special needs are planned for carefully, with individual programmes drawn up by the class teacher in conjunction with the SENCO. There is a shared expectation that children with additional needs are provided with the appropriate support to access challenging learning, enabling progress from their starting points.

Equal opportunities

Talbot Primary School is an advocate of equal opportunities. Our values are set out in the Equal Opportunities Policy.

Monitoring and review

The Subject Leader for computing is responsible for implementing and monitoring this policy. This includes monitoring planning. Their work will be subject to annual review by the Head Teacher, as part of the on-going Performance Management arrangements. The subject is also reviewed annually, by a named Governor; their findings are shared in subsequent Governor meeting, in the School Improvement Sub-Committee.

- Regular monitoring of all aspects of computing informs the subject leader and, in turn, the School Improvement Plan.
- The subject leader is responsible for supporting colleagues in the teaching of computing, for being informed about current developments in the subject, and for providing a strategic lead and direction for the subject in the school.

Any information that needs to be recorded will be done so on the school's online reporting facility.

Cross curricular Links

- The teaching of computing at Talbot extends far beyond the discrete computing lessons. Key themes are delivered and reinforced in other areas of the curriculum such as PSHE, class and whole school assemblies, along with themed weeks. These can be accessed via the school's long term plans.
- Where appropriate, computing should be incorporated into other areas of the curriculum providing opportunities to apply key skills and see skills used in a variety of different contexts.
- Computing should be used to support learning in other subjects as well as developing computing knowledge, skills and understanding.

Learning styles and the learning environment

- The Computing suite will be a stimulating learning environment linked to the children's learning.
- Long term planning and teaching takes account of differentiation and progression.
- The scheme ensures there is appropriate levels in challenge in every lesson including prompts, vocabulary, sentence stems. Given tasks build on previous learning to ensure challenge increases across year groups and Key Stage.
- Teachers share key vocabulary at the start of each topic which is referred to throughout the unit.
- Open questions will be developed to challenge children's thinking and learning, encouraging the principles of talk matters.
- Independent learners will have access to a variety of resources and encouraged to reflect on the choices that they have made.
- Ipads will be used to support teaching and learning in the classroom in other areas of the curriculum to encompass key skills.

Virtual Learning Platform and related websites

Tapestry (Early Years)

Tapestry an online application that is used to store photographic and anecdotal evidence. It builds a record of a child's experiences and journey through their early years, using an online learning journal. All information held in the platform is kept securely, and can be downloaded and shared as required. Tapestry enables regular communication between staff and parents.

DB Primary

Individual log in details are provided to pupils from Reception. DBPrimary is introduced formally from Reception. This provides a secure area for pupils to socialise and share work and provides a controlled introduction to social networking (including e-mail). Pupils are taught about appropriate communications. DB Primary can be monitored by staff and the appropriate action taken, if an incident is reported. Pupils who leave the school and Year 6 pupils who move onto high school will have their accounts deactivated upon leaving.

Purple Mash

Purple Mash is a cross-curricular website which can be accessed both at school and at home. It provides a safe environment that enables children to explore and enhance their knowledge in fun and creative ways. Each child has a personalised log in.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Online Communication Policy
- PSHE Policy
- Guidance for Safer Working Practices
- Responsible use agreement and acceptable use

Appendix 1 - Acceptable Use Policy for Staff

The school's Acceptable Use Policy for the internet and digital devices has been drawn up to protect both staff and the school. Computer systems owned by the school are primarily made available to staff to enhance their professional activities (including teaching, research, administration and management). The school also allows limited personal use in line with this policy. This refers to school laptops, I pads, digital devices and mobile phones.

The school reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited. Neither the school nor the Local Authority will be liable under any circumstances for any injury, distress, loss or damage which may arise directly or indirectly from the use of the Internet facilities, the use of e-mail, or from other person's unauthorised use of those facilities or e-mail.

Professional Use:

- Staff should only ever use a school phone/contact when contacting parents or carers

- Internet use should be appropriate to staff professional activity or student's education; users will recognise when materials are inappropriate and should expect to have their access removed if used improperly.

- The viewing and/or downloading of any radical/extremist, sexist, racist, pornographic, anti-Semitic, indecent or abusive images, text or sound files is strictly forbidden.

- Automatic updates, which are updated by the school network, should all be accepted. If staff have any concerns about downloading programmes or updates, it is their responsibility to seek advice from either from the technician or computing leader.

- Permission will be sought from staff, pupils and parents before any personal data, i.e. names and photographs, are published on the school website in accordance with GDPR procedures; **specific permission will be sought before any personal data is to be published on other websites.** Permission is stored through SIMS. Permission is not required for DB Primary as this is a closed network.

- Users are responsible for the e-mails they send and for contacts made that may result in e-mail being received. It is strongly advised that the same professional levels of language and content should always be applied in e-mails as for letters or other media, **particularly as e-mail is often forwarded**.

- Users should only use the school approved e-mail system for any professional business, including communication with parents and other agencies. Staff should only send emails from their school based address.

- Information about the school can be sent in cases **where staff are certain it is fit for public knowledge.**

- Devices that do not contain up to date anti-virus software (including USB devices) should not be connected to the network.

- All digital devices are the property of Talbot Primary School and are for use **only** by you, support staff and pupils in your class. They must not be loaned to other adults or pupils without agreement from the Headteacher.

- Insurance cover provides protection from the standard risks whilst the mobile device is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave digital devices unattended and it is stolen you could be held responsible for its replacement.

- Loss or damage of a device should be reported to the head teacher, computing leader or business manager immediately.

- When left unattended, digital devices should be locked in a secure cupboard.

- Digital devices are expensive and fragile items and their use must be supervised at all times. They should only be used under adequate supervision and when the teacher believes that all pupils present are capable of using them sensibly.

- Staff should not use personal digital cameras or mobile phones to take, edit or store images. All staff are advised to access school based Wi-Fi when accessing their personal devices in school in accordance with our safeguarding procedures. Where staff use their own data to access Wi-Fi in school they are reminded that their conduct must continue to meet expectations as set out in the agreed Guidance for Safer Working Practices policy.

- Staff should save all media (photos, videos) to the media drive on the shared network.

- Activity that threatens the integrity of the school systems, or that attacks or corrupts other systems, is forbidden; if such material is detected the school reserves the right to print and use the files as evidence for disciplinary action.

If a staff member accesses inappropriate material by accident, they should speak to the named person, who is responsible for Online Safety, as soon as is reasonably possible. At Talbot Primary School, this is the Headteacher, or Deputy in their absence.

Personal Use:

- **Where staff wish to use their computers for personal use, the same standards and rules apply as for professional use; however, the following additional guidelines must also be adhered to:**

- The school expects staff to make careful decisions, **as professionals who are representing the school,** about their personal Internet use. **Where staff are in any doubt as to the suitability of material, they are expected to err on the side of caution.** This is also in accordance with key safeguarding policies in school, in particular Guidance for Safer Working Practices

- Staff **are** permitted to use their computers for the following purposes: to send their own personal data, including e-mails; to make personal purchases, to make contracts and payments, to organise their banking affairs and to advertise. **Again, all activities are undertaken at the staff members own risk.**

- Staff **are not** permitted to use their computers for the following purposes: the downloading of screen savers, downloading or installing games, posting anonymous messages, social networking sites, forwarding chain letters, gambling and/or political purposes. The intellectual property rights with respect to copyright must be followed.

- Members of staff should never engage in discussions about school on social media networks, such as Facebook, Instagram, Whatsapp, etc. This is likely to be deemed as a breach of confidentiality and could result in disciplinary action. Staff should never use their phone during teaching time or use their device to take pictures in school.

- Contact with parents must remain via school e-mail accounts and contact with children must be via DB primary. This is also in accordance with key safeguarding policies in school, in particular Guidance for Safer Working Practices

- The deliberate, inappropriate use of the Internet will be seen as an extremely serious matter and is likely to result in disciplinary action.

- Staff requesting Internet access must sign a copy of this Acceptable Use Policy and return it to the office. Staff should be aware that Internet access can be monitored and reported to the Head teacher.

Staff must take great care for digital devices which they take home, as they are responsible for them. For example, laptops should not be left unattended in vehicles or in places where they are visible - as this would likely invalidate any insurance claim.

Full name ____

Post ___________________________________

I have read and understand the school's Internet and Digital Device Acceptable Use Policy.
I acknowledge that contravention of these rules may result in formal, disciplinary action.
I consent to the monitoring and auditing of my school e-mails, internet access and school laptop.

Signed ____

Date ___________________

Appendix 2 - Acceptable Use Policy for Visitors

In this instance, visitors refers to long term visitors to the school such as long term supply, student teachers or long term volunteers who have access to computing equipment. The school's Acceptable Use Policy for the internet and digital devices has been drawn up to protect both visitors and the school. Computer systems owned by the school are primarily made available to volunteers to enhance their professional activities (including teaching, research, administration and management). The school also allows limited personal use in line with this policy. This refers to phones, school laptops, I-pads and digital devices. The school reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited. Neither the school nor the Local Authority will be liable under any circumstances for any injury, distress, loss or damage which may arise directly or indirectly from the use of the Internet facilities, the use of e-mail, or from other person's unauthorised use of those facilities or e-mail. Visitors should use the supply teachers log on which can be obtained from the Computing Co-ordinator or Mrs Hogg.

Professional Use:

- Volunteers should never contact parents/carers or children using either their own device or that which belongs to school

- Internet use should be appropriate to staff professional activity or student's education; users will recognise when materials are inappropriate and should expect to have their access removed if used improperly.

- The viewing and/or downloading of any radical/extremist, sexist, racist, pornographic, anti-Semitic, indecent or abusive images, text or sound files is strictly forbidden.

- Internet use should be appropriate to a volunteer's professional activity or student's education; users will recognise when materials are inappropriate and should expect to have their access removed if used improperly.

- The viewing and/or downloading of sexist, racist, pornographic, indecent or abusive images, text or sound files is strictly forbidden.

- Automatic updates, which are updated by the school network, should all be accepted. If volunteers have any concerns about downloading programmes or updates, it is their responsibility to seek advice from either from the technician or computing leader.

- Permission will be sought from visitors, pupils and parents before any personal data, i.e. names and photographs, are published on the school website in accordance with GDPR protocols; **specific permission will be sought before any personal data is to be published on other websites.** Permission is stored through SIMS. Permission is not required for DB Primary as this is a closed network.

- Users are responsible for the e-mails they send and for contacts made that may result in e-mail being received. It is strongly advised that the same professional levels of language and content should always be applied in e-mails as for letters or other media, **particularly as e-mail is often forwarded**.

- Information about the school can be sent in cases **where volunteers are certain it is fit for public knowledge.**

- Devices that do not contain up to date anti-virus software (including USB devices) should not be connected to the network.

- All digital devices are the property of Talbot Primary School and are for use **only** by you, support volunteers and pupils in your class. They must not be loaned to other adults or pupils without agreement from the Headteacher. All volunteers should refrain from when accessing their personal devices during teaching time.

- Insurance cover provides protection from the standard risks whilst the mobile device is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave digital devices unattended and it is stolen you could be held responsible for its replacement.

- Loss or damage of a device should be reported to the head teacher, computing leader or business manager immediately.

- When left unattended, digital devices should be locked in a secure cupboard.

- Digital devices are expensive and fragile items and their use must be supervised at all times. They should only be used under adequate supervision and when the teacher believes that all pupils present are capable of using them sensibly.

- Volunteers should not use personal digital cameras or mobile phones to take, edit or store images. All volunteers should access school based Wi-Fi when accessing their personal devices in school in accordance with our safeguarding procedures

- Activity that threatens the integrity of the school systems, or that attacks or corrupts other systems, is forbidden; if such material is detected the school reserves the right to print and use the files as evidence for disciplinary action.

If a volunteer accesses inappropriate material by accident, they should speak to the named person, who is responsible for Online Safety, as soon as is reasonably possible. At Talbot Primary School, this is the Headteacher, or Deputy in their absence.

Personal Use:

- **Where volunteers wish to use their computers for personal use, the same standards and rules apply as for professional use; however, the following additional guidelines must also be adhered to:**

- The school expects volunteers to make careful decisions, **as professionals who are representing the school,** about their personal Internet use. **Where** volunteers **are in any doubt as to the suitability of material, they are expected to err on the side of caution.** This is also in accordance with key safeguarding policies in school, in particular Guidance for Safer Working Practices

- Volunteers **are** permitted to use their computers for the following purposes: to send their own personal data, including e-mails; to make personal purchases, to make contracts and payments, to organise their banking affairs and to advertise. **Again, all activities are undertaken at the volunteer's own risk.**

- Volunteers **are not** permitted to use their computers for the following purposes: the downloading of screen savers, downloading or installing games, posting anonymous messages, social networking sites, forwarding chain letters, gambling and/or political purposes. The intellectual property rights with respect to copyright must be followed.

- Members of volunteers should never engage in discussions about school on social media networks, such as Facebook, Instagram, Whatsapp, etc. This is likely to be deemed as a breach of confidentiality and could result in immediate termination of the volunteer arrangement. This is also in accordance with key safeguarding policies in school, in particular Guidance for Safer Working Practices

- The deliberate, inappropriate use of the Internet will be seen as an extremely serious matter and is likely to result in disciplinary action.

- Volunteers requesting Internet access must sign a copy of this Acceptable Use Policy and return it to the office. Volunteers should be aware that Internet access can be monitored and reported to the Head teacher.

Full name :
Post :

I have read and understand the school's Internet and Digital Device Acceptable Use Policy.
I acknowledge that contravention of these rules may result in formal, disciplinary action.
I consent to the monitoring and auditing of my school e-mails, internet access and school laptop.

Signed:
Date :

Appendix 3 - Responsible Use Agreement
Key Stage Two Pupils

Dear Parent/Carer,

As part of the National Curriculum, we provide supervised access to the internet in Key Stage 2. We believe this enhances learning opportunities and helps develop important computing skills.

Although there can be concerns about pupils having access to undesirable materials, we are taking a number of positive steps to deal with this risk in school.

- Firstly, your child will only be allowed to use the internet under adult supervision.
- Secondly, we are making great efforts to teach your children about safe internet use so they can protect themselves.
- Finally, incidents will be monitored by their teachers and reported to school governors and myself on a regular basis.

Attached is a copy of our home/school agreement entitled “How to Use the Internet Safely at School”, which we feel is suitable for the way we now use computers, laptops and iPads. It is a code of conduct that we would like you to read and discuss with your child.

Should you wish to find more information about online safety, you can access this advice via the school website (Computing and Online Safety) Also, we will update you on any key online safety messages in our school monthly newsletter for parents and carers.

Yours faithfully,

Parm Gill
Headteacher

How to use the internet safely in school

Rules for all Key Stage Two pupils

The school has computers and internet access to help our learning. Key Stage Two pupils will only be allowed to use the internet, if they agree to the following rules which are designed to keep them safe.

- I will ask permission from an adult before using the internet.
- I will use only my own login name and password, which I will keep secret.
- I will use the computers for school work and homework only, unless told otherwise.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I will only access appropriate websites that I know. If I am unsure whether a website is appropriate, I will ask the teacher first.
- I will only e-mail people I know, or people my teacher has approved.
- The messages I send will be polite and sensible.
- I will never give my full name, home address or phone number, or any other personal information to anybody over the internet.
- I will never give the full name, home address or phone number, or any other personal information about another pupil to anybody over the internet.
- I will never arrange to meet anyone over the internet.
- I will never send a photograph of myself or another person over the internet without checking with my parents or teacher first.
- I will not access other people's files, unless I have permission from a teacher.
- I will remember to LOG OUT when I have finished my session.
- I understand that the school may check my computer files and will monitor the internet sites I visit.

If you break a rule by accident, it is important that you tell a teacher as soon as possible. If you deliberately break these rules, you could be banned from using the internet for a period of time and/or your parents could be told.

Signed (pupil): **Date:**