Federation of Boldmere Schools

National Curriculum objectives:

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 precise and unambiguous instructions
- Create and debug simple programs
- Use logical reasoning to predict the behaviour of simple programs
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content
- Recognise common uses of information technology beyond school
- 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.

Key stage 2

Pupils should be taught to:

1. Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
2. Use sequence, selection, and repetition in programs; work with variables and various forms of input and output
3. Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
4. 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
5. Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
6. Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
7. Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

NC link	Skills	Key vocabulary in bold Boldmere Blue Curriculum *Green refers to the Computing Knowledge organisers.*			
		Year 3	**Year 4**	**Year 5**	**Year 6**
Computer Science- Theory and Programming					
1.	KS1 Prior learning: *Create and debug simple programs* Make and debug programs that accomplish specific goals **All Year groups to refer to Computer Science Theory- when teaching the programming. **	Use **block-based coding** to create an end goal (e.g. an **animation**), whilst spotting and correcting mistakes as they go. *Look at Writing Algorithms.* Scratch Stop motion Turtle logo (turtleacadmy website)	Use **block-based coding** to create an end goal, whilst spotting and correcting mistakes as they go. Scratch Matrix (physical outcome) Pro-bots	Use a **given brief** to design their own program to achieve the **specific goal**. Kodu Flowol Scratch- Intro to programming with numbers.	**Design** their own program to achieve the **specific goal**. *Look at the Systems life cycle.* Kodu Micro bit Scratch- Programming with random numbers

1 and 3	KS1 Prior learning: *Use logical reasoning to predict the behaviour of simple programs* Decompose a given program into smaller parts/ Make and debug programs that accomplish specific goals	**Break a program up** into main areas (e.g. In an **animation**, you need to program the sprites and backgrounds.)	**Break a program up** into main areas (e.g. Using matrixes, what steps will you need to do create an **output**.)	Use **coding** to create an **end goal** (e.g. a game). *Look at flowcharts of Control systems.*	Use **coding** to create an **end goal, whilst spotting and correcting most mistakes as they go.**
2.	KS1 Prior learning: *Use logical reasoning to predict the behaviour of simple programs* Create programs that use sequence Use selection and variables in programs	Write a program that uses a **sequence** to produce an output.	Program a Scratch Matrix to receive an **input** and show an **output.** *Begin to look at Conditional Events (Selection) with support from an adult.*	Use selection in **block-based coding** (e.g. Using an "If" function to end the game if the boat goes out of the water) and **variables** (E.g. to create a timer/scoring system). *Look at programming with numbers.*	Understand what a **variable** is and uses them in their **own program**. E.g. to create a timer in a game. *Look at Random numbers.*
3	KS1 Prior learning: *Understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions* Explain how algorithms work in a given program	**Talk through** their own code to **explain why** it does what it does.	Use **repeat blocks of code** (e.g. in Logo software to draw a simple shape.) Probots *Look at On- Screen Turtle Programming*		Program a Micro:Bit to use an **input and show multiple outputs** of a real life system e.g. An air raid warning system.

Information Technology					
6	KS1 Prior learning: *Use technology purposefully to create, organise, store, manipulate and retrieve digital content* Select, use and combine software or internet services from multiple devices to create content that accomplish specific goals	Create content **in groups** using multiple pieces of software to **accomplish** a given goal. *Look at Manipulating Text and photo editing* Word Photo editing	Create content using multiple pieces of software to **accomplish** a given goal. *Look at features of a neat document and video editing.* Publisher Green screen by Do Ink I can Animate- Video Editing	Combine the appropriate software to achieve a **specific goal**. *Look at Creating a Presentation and Spreadsheets.* PowerPoint presentation Ipads- Vlogging Ipads- Blogging Excel	Combine the appropriate software to achieve a **specific goal,** explaining the benefits and drawbacks of another method they could have used. *Look at Creating a Website and Databases.* Google Schudio Padlet Excel
6.	Type at a pace of 10 words a minute using the shift key to add punctuation and capitals (Y3/4) Use both hands to type at a pace of 15 words a minute using the shift key to add any letter/symbol (Y5/6)	Confidently use the **shift key** to add punctuation/capitals whilst maintaining a speed of 10 words a minute	**Confidently use most punctuation** and all letters whilst maintaining a speed of 15 words a minute.	Type using the **appropriate hands/fingers** to achieve a speed of 15 words a minute	**Input any letter/symbol on the keyboard using both hands** at a speed of 20 words per minute.

Digital Literacy					
4	KS1 Prior learning: *Recognise common uses of information technology beyond school* Use a computer network for communication	**Send and receive** communication. Email	**Send and receive** communication. Face time/ Skype Twitter Email	Work collaboratively with a team to complete a group project. *Look at E-commerce and Vlogging* Blogging Vlogging Twitter Social media-awareness	Work collaboratively with a team to complete a group project. *Look at E-commerce and Vlogging* Vlogging Twitter Social media-awareness
7.	KS1 Prior learning: *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.* Use technology safely, respectfully & responsibly by recognising acceptable/unacceptable behaviour	Recognise what is **acceptable/unacceptable** behaviour from a given scenario. *Look at Comparing online behaviours.* Social media input *See additional E-safety document below*	Suggest examples of **acceptable/unacceptable** behaviour online. *Look at Comparing online behaviours and age restrictions.* Social media input *See additional E-safety document below*	Understand the consequences of unacceptable behaviour on **online platforms** (E.g. fines/prison sentences for **trolling**/online verbal abuse) *Look at online manipulation tactics* Social media input *See additional E-safety document below*	Understand how to use the internet responsibly including the use of **copyright.** *Look at online Personal Information and Privacy.* See questions to consider below

7.	KS1 Prior learning: *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.* Identify inappropriate/unacceptable content and know how/where to report it to	Recognise what is **inappropriate content** from a given scenario and explain what they could do to stop it. *Look at Comparing online behaviours.* Social media input *See additional E-safety document below*	Come up with their own ideas of **inappropriate content** and explain/show someone else what they should do to report it. *Look at Comparing online behaviours.* Social media input *See additional E-safety document below*	Understand multiple ways to report inappropriate content outside of school. Social media input *See additional E-safety document below*	Understand how to check who someone is online and how to report something suspicious. Social media input *See additional E-safety document below*
5.	KS1 Prior learning: *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.* Selective when using researched digital content/ Understand how search technologies select and rank results	In groups, use **search engines** (e.g. Google) to find specific content and select a good website for this. *Look at finding helpful search results.* See questions to consider below	Explain how **web crawlers** & **ranking** points work. *Look at interpreting URLs.* *See additional E-safety document below*	Check the reliability of an online source and use multiple sites to ensure the use of **unbiased content.** *Look at tips for effective web searching.* *See additional E-safety document below*	

Additional E-safety to consider

In line with the 'Teaching online safety in school' June 2019 document, when you are teaching the 'digital literacy' skills, please consider the following questions. It does not matter if we repeat any of the information below, as its important information the children need to hear repeated.

How to evaluate what they see online
- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?
-

How to recognise techniques used for persuasion
- Discussing the ways in which someone may put themselves at risk online,
- Discussing risks posed by another person's online behaviour,
- Discussing when risk taking can be positive and negative,
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,

How and when to seek support

- Helping them to identify who trusted adults are,
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Digital content- Knowing what happens to information, comments or images that are put online. Teaching could include:

- What a digital footprint is, how it develops and how it can affect future prospects such as university and job applications,
- How cookies work,
- How content can be shared, tagged and traced,
- How difficult it is to remove something a user wishes they had not shared,
- Ensuring pupils understand what is illegal online, especially what may in some cases be seen as "normal" behaviours, for example youth-produced sexual imagery (sexting). This could include copyright, sharing illegal content such as extreme pornography or terrorist content as well as the illegality of possession, creating or sharing any explicit images of a child even if created by a child.

Disinformation, misinformation and hoaxes- Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.
Teaching could include:

- Disinformation and why individuals or groups choose to share false information in order to deliberately deceive,
- Misinformation and being aware that false and misleading information can be shared inadvertently,
- Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons,
- Explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online,
- How to measure and check authenticity online,
- The potential consequences of sharing information that may not be true.

Fake websites and scam emails- Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other gain.

Teaching could include:
- How to look out for fake URLs and websites,
- Ensuring pupils understand what secure markings on websites are and how to assess the sources of emails,
- Explaining the risks of entering information to a website which isn't secure,
- What to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available.

Year 5 and 6
Password phishing- Password phishing is the process by which people try to find out your passwords so they can access protected content.
Teaching could include:
- Why passwords are important, how to keep them safe and that others may try to trick you to reveal them,
- Explaining how to recognise phishing scams, for example those that seek to gather login in credentials and passwords,
- Importance of online security to protect against viruses (such as keylogging) that are designed to access/steal/copy passwords information,
- What to do when a password is compromised or thought to be compromised.

Year 3, 4, 5, 6
Personal data- Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming'.
Teaching could include:
- How cookies work,
- How data is farmed from sources which look neutral, for example websites that look like games or surveys that can gather lots of data about individuals,
- How, and why, personal data is shared by online companies. For example data being resold for targeted marketing by email/text (spam),
- How pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential,
- The rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR),
- How to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time.

Persuasive design - Many devices/apps/games are designed to keep users online for longer than they might have planned or desired.

Teaching could include:
- Explaining that the majority of games and platforms are businesses designed to make money. Their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue,
- How designers use notification to pull users back online.

<u>Privacy settings</u>- Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.
Teaching could include:
- How to find information about privacy setting on various sites, apps, devices and platforms,
- Explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate.

<u>Targeting of online content. Including on social media and search engines-</u> Much of the information seen online is a result of some form of targeting.
Teaching could include:
- How adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts,
- How the targeting is done, for example software which monitors online behaviour (sites they have visited in the past, people who they are friends with etc) to target adverts thought to be relevant to the individual user,
- The concept of clickbait and how companies can use it to draw people onto

When teaching how to stay safe online, consider the following;

The potential harms or risk	Description/ questions to consider
Abuse online	- Explain what types of abuse happen online- trolling, bullying, harassment, intimidation - Explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail - How to respond to online abuse

	- How to respond when the abuse is anonymous - Discussing the potential implications of online abuse - Being clear what good online behaviours do and don't look like
Challenges	- Explaining what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal - How to assess if the challenge if safe or harmful - Explaining to pupils it is ok to say no and not take part - Understanding the importance of telling an adult
Fake profiles	Everyone online isn't who they say they are; - Some profiles may be people posing as others - How to look out for fake profiles
Unsafe communication	Knowing different strategies for staying safe when communicating