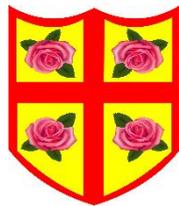


**ST GEORGE AND ST TERESA  
CATHOLIC PRIMARY SCHOOL**



**Online Safety and Acceptable  
Use Policy**

**Ratified February 2019**

# **CONTENTS**

- 1. Mission Statement**
- 2. School Aims**
- 3. Rationale**
- 4. Aims**
- 5. Objectives**
- 6. Definitions**
- 7. Responsibilities**
- 8. Procedures and Practice**
- 9. Equal Opportunities and SEND**
- 10. British Values**
- 11. Glossaries and Appendices**

## **1. Mission Statement**

St George & St Teresa School is a Catholic School where we show love and care to all members of the community.

It is a place where the Trinity is central to our lives; where we pray together, praising Almighty God, learning about Him and growing closer to Him.

It is a place where we work together, living our faith, and learning together, sharing and developing our knowledge, skills and understanding through all aspects of the curriculum.

It is a place where we endeavour to live as Christians in a multicultural, multi-ethnic society.

## **2. School Aims**

To promote the Christian growth of the children in accordance with the teachings of the Catholic Church and to successfully embrace the Mission Statement.

To provide a broad, balanced and exciting curriculum that meets the requirements and needs of all the children and to ensure that all children achieve the highest possible attainments in relation to their abilities across the full range of learning experiences.

To develop creative, open, inquisitive, lively, rich and discerning minds, physical skills, ambition and a positive response to challenge.

To provide a positive climate which encourages high standards of behaviour and develops children's self-discipline and a respect and tolerance for others and their property.

To provide a happy, safe, healthy, stimulating and secure learning environment which develops children's self-confidence, independence and self-esteem.

To help children understand the world in which they live and to develop a full range of skills necessary for their next step in their lifelong learning and to become responsible members of society in a rapidly changing world.

To establish an environment of collegiality within which all the members of the school family i.e. children, parents, teaching and non-teaching staff, Governors, Parish, Local Authority, external agencies, the wider community and other schools, can work collaboratively to successfully achieve these aims.

### 3. Rationale

This policy applies to all members of our school community including: staff, pupils, volunteers, parents/carers, visitors and community users who have access to and are users of school ICT systems, both in and out of the school.

We recognise that online safety is a fundamental part of safeguarding our children and our policy is integrated with our behaviour, safeguarding and anti-bullying policies.

### 4. Aims

This policy aims:

- to help our pupils to develop the skills to use information wisely and well.
- to help our pupils avoid becoming victims of crimes such as identity theft and fraud.
- to help our pupils avoid embarrassment or humiliation, including cyberbullying.
- to help to keep our pupils safe from predatory adults.
- to help our pupils to avoid harmful behaviours such as obsessive use of new technologies or digital games.
- to help our pupils to avoid physical danger.
- to help our pupils to resist extremist views.
- To help our pupils from being exploited.

### 5. Objectives

- Online Safety is embedded in all aspects of technology use.
- Pupils are informed of the appropriate actions to take if faced with an online safety issue.
- To work with parents and carers to embed a culture of online safety in the wider community.

### 6. Definitions

**Online Safety:** Online Safety is a term which means not only accessing the internet through desktop computers but other ways in which young people communicate using electronic media, e.g. mobile phones, gaming platforms or other handheld devices. It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

The term Online Safety therefore covers a broad range of aspects including physical safety, emotional wellbeing, legal aspects such as copyright and technical issues such as filtering.

See Glossary for Computing definitions.

## **7. Responsibilities**

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

### Designated Member of Staff:

- Mr Foxon- Headteacher
- Mrs N. Wright - Deputy Headteacher
- Mrs Packwood, Dragons Manager

### Computing Subject Leader:

- Mrs C. Fahy

## **Governors**

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, who oversees Safeguarding, also incorporates all aspects of Online Safety. The role of this Governor will include:

- regular meetings with the Computing Subject Lead and/or Designated Senior Person
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

## **Headteacher and Senior Leaders**

- The Headteacher has a duty of care 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 Computing subject lead and Designated Senior Person.
- The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. See flow chart on dealing with online safety incidents – Appendix 1.
- The Headteacher/Senior Leadership Team are responsible for ensuring that the Computing Subject Lead/Designated Senior Person and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher will receive regular monitoring reports from the Computing Subject Lead/ Designated Senior Person.

### **Computing Subject Lead**

- leads on online safety issues
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and/ or other relevant bodies
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Governors to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

### **Technician**

The school technician is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority Policy/Guidance that may apply.
  - that users may only access the networks and devices through a properly enforced password protection device.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network/internet/ remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ Computing Lead/Designated Senior Leader for investigation/action/sanction.
- that monitoring software/systems are implemented and updated.

### **Teaching and Support Staff**

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement . (Appendix 2)
- they report any suspected misuse or problem to the Headteacher/Computing Lead/Designated Senior Person for investigation/action/sanction.

- all digital communications with parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and agree to follow the online safety and Pupils Acceptable Use Agreement – these are found in Home School Organisers. (see also Appendix 4.)
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed).
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Child Protection/Safeguarding Designated Person-**

Mr D. Foxon and Mrs N. Wright

The Child Protection/Safeguarding Designated Person should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

### **Pupils:**

- are responsible for using the school digital technology systems in accordance with the Pupils Acceptable Use Agreement – these are found in Home School Organisers. (see also Appendix 4.)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so – by informing an adult in school as soon as possible.
- They should also know and understand procedures on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies both in and out of school.

### **Parents/Carers**

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

- digital and video images taken at school events.
- their children's personal devices in the school (where this is allowed)

### **Community Users**

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. See Appendix 3

## **8. Procedures and Practice**

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum that is delivered is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be helped to understand the need for the Pupils Acceptable Use Agreement in their Home School Diary (KS1 and KS2) and be encouraged to adopt safe and responsible use both within and outside school.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technician (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be communicated with the Headteacher and the Computing Lead, with clear reasons for the need.

### **Education – Parents / Carers**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day

### **Education & Training – Staff / Volunteers**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Planned, quality time during staff meetings to provide online safety training and updates will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The DMS/Computing Lead (or other nominated person) will receive regular updates through attendance at external training events
- This policy and its updates will be presented to and discussed by staff in staff meetings.

- The Computing Lead will provide advice / guidance / training to individuals as required.

### **Training – Governors**

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

### **Technical – Infrastructure / Equipment, Filtering and Monitoring**

St George and St Teresa School have a managed ICT service provided by an outside contractor; however we recognise that it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school's Online safety Policy and Acceptable Use Agreements.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements outlined in Local Authority guidance
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS1 and above) will be provided with a username and secure password. Users and teaching staff are responsible for the security of their username and password.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher
- The technician – along with the Headteacher - is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.

- School technicians regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Procedures are in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) – they have limited access to systems.

## **Mobile Technologies**

St George and St Teresa School do not operate a Bring Your Own Device policy. Pupils are not allowed to bring their own devices from home. Personally owned mobile technology might include: smartphone, tablet, notebook / laptop, smart watch or other technology that usually has the capability of utilising the school’s wireless network.

The functionality of smart watches varies – from bring a fully functioning smart phone to solely being a health monitor. Solihull Local Authority release advice to schools in January 2019 that states:

*‘We believe the most significant safeguarding risk is from pupils having the ability to record themselves, other pupils and staff, which could even be done covertly.’*

*‘We believe that the safest and most effective response for schools is to tell parents that pupils are not allowed to wear smart watches during the school day for the same reasons that pupils are not allowed to use mobile phones during the school day’*

See Appendix 5

## **Use of Digital and Video Images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, we request that these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images – parents / carers give their consent to do so when joining the school.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy. (see appendix for template policy)
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual

clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.

- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- School has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

## **Communications**

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. (Online Safety BOOST includes an anonymous reporting app Whisper – <https://boost.swgfl.org.uk/>)
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above can be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks.	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

Pornography				X	
Promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. See Appendix 1.

## Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may

be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

• Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
- Police involvement and/or action

• If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

## School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

### 9. Equal Opportunities and SEND

At St George & St Teresa school we provide for equal opportunities in Computing and take into account culture, gender and special educational needs and disabilities in all our planning and teaching. In all classes there are children of differing ability. We recognise this fact and provide suitable learning opportunities for all children by matching the challenge of the task to the ability of the child. We achieve this through following the principles laid down in the National Curriculum and using a range of strategies including:

- Setting suitable learning challenges
- Responding to pupils' diverse learning needs by differentiating tasks, grouping and pair working
- Setting open ended investigations and analysis
- Linking IEPs, needs based plans or other individual programmes, where appropriate to suitable learning outcomes from the National Curriculum
- Overcoming potential barriers to learning and assessment for individuals and groups of children.
- Use of suitable resources to support SEND pupils

### 10. British Values

The DfE have reinforced the need *“to create and enforce a clear and rigorous expectation on all schools to promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.”*

The Government set out its definition of British values in the 2011 Prevent Strategy, and these values have been reiterated this year (2014). These values fall into the following broad areas;

- Democracy
- The rule of law
- Individual liberty
- Mutual respect
- Tolerance of those of different faiths and beliefs

Please see our British Values statement and overview of activities.

## 11. Glossaries and Appendices

### Glossary

This is a glossary of some of the key terms encountered in the new Computing curriculum

Abstraction	Digital Content	Output	Software
Algorithm	Evaluation	Pattern recognition	Variables
Computer networks	Generalisation	Program	World Wide Web
Computational thinking	Information	Repetition	
Control	Input	Search	
Data	Internet	Selection	
Debug	Language	Services	
Decomposition	Logical Reasoning	Simulation	

### Abstraction

Abstraction is one of the 6 key concepts of computational thinking and is the process of simplifying complex information to give only the amount required . When we are asked how old we are, we give our answer in years not in years, weeks and days or just in days. When writing shopping lists, we might write fruit & veg understanding that this represents the products we routinely buy. In class we might ask children to record the plot of a short story in a storyboard. In doing this they are selecting only the information that is needed as disregarding that which they deem unnecessary. Children should understand that the programs they write are an abstraction, behind this language exists a more complex set of instructions that gets e.g. the the turtle to draw the square.

### Algorithm

An algorithm is a step by step process by which a desired outcome is achieved. Algorithms can be constructed using words, images, symbols, or a programming language. We all use algorithms on a daily basis, when classes line up for assembly, when we follow a cooking recipe or when build lego models or IKEA furniture. When creating their own algorithms, pupils need to identify what the goal is and sequence their instructions in the correct order.

### Computer networks

The computers and the connecting hardware (wifi access points, cables, fibres, switches and routers) that make it possible to transfer data using an agreed method ('protocol'). Computers and wireless devices that are connected to the same server and the hardware that allows these connections (wifi access points, cables, fibres, switches routers) are part of a computer network. Theses devices are able to exchange data with each other using an agreed method ('protocol'). A small network

such as one at home or at school is known as a local area network (LAN). When smaller networks join together a larger, wide area network (WAN) is formed. The biggest WAN is the internet.

## **Computational thinking**

Computational thinking allows us to develop skills and techniques to help us solve problems effectively, with or without the aid of a computer.

### **Control**

When we program computers to achieve outcomes that are not on the screen but on an attached device we are using control. This might be programming motors or a set of lights to come on in a certain sequence. Control also involves using devices connected to the computer to sense conditions and execute programs when these conditions are met. Pedestrian crossings are not activated until a button is pressed then a program will run which will stop the traffic and allow the pedestrians sufficient time to cross safely.

### **Data**

A structured set of binary numbers, representing digitised text, images, sound or video, which can be processed or transmitted by a computer.

### **Debug**

When a program doesn't achieve the desired outcome it is because we have not instructed the computer correctly. The mistake we have made is referred to as a bug; the process by which the bug is located and corrected is known as debugging. A risotto recipe which instructs one to add 2 tbps of salt will not produce the delicious meal that was expected. By debugging this algorithm and replacing with 2 tsp the algorithm has been debugged and the desired outcome has been reached. We should encourage children to use logical reasoning when debugging. When programming a quiz, we might end up with a message telling us that the incorrect answer we have given is correct. This should lead us to think that the bug might be in the selection statements for that given answer.

### **Decomposition**

Decomposition is one of the 6 key concepts of computational thinking and is concerned with breaking a problem or a system down into its parts. Pupils have plenty of experience of this in primary schools: they partition numbers when adding;

they plan settings, characters and a 5 part plot before story writing, they identify materials, equipment and processes needed before making DT products. When writing more complex programs, children should be encouraged to think about the different things that their program needs to do in order to achieve its goal. A simple maze game in scratch might need: a maze; a sprite to move around the maze; the means by which to move the sprite; a timer; selection statements to define what happens if the maze wall is touched. By identifying such criteria first, children will then understand the different parts their program will need to incorporate.

## **Digital content**

The materials that pupils produce or view when they are using computer devices are known as digital content. These can be text based documents, images, podcasts, graphic models, videos, animations or multimedia presentations in which several of these are combined. The children in our classes have been producing digital content for a while, we just didn't know it was called that.

## **Evaluation**

Evaluation is one of the 6 key concepts of computational thinking and is concerned with making judgements, in an objective and systematic way whenever possible.

## **Generalisation (also called pattern recognition)**

Generalisation is one of the 6 key concepts of computational thinking.

## **Information**

The meaning or interpretation given to a set of data by its users, or which results from data being processed.

## **Input**

Data provided to a computer system, such as via a keyboard, mouse, microphone, camera or physical sensors.

## **Internet**

The global collection of computer networks and their connections, all using shared protocols (TCP/IP) to communicate.

## **Language**

When creating programs children are working with a programming language. This language will be made up of a series of predetermined symbols or words which have to be used with the correct syntax. Although the words or symbols might be similar from one application to the next, the instructions might yield different results. For example a right arrow on a beebot turns the device 90 degrees clockwise, whereas a right arrow on kodable moves the character forward along the screen. Similarly, we might be trying to achieve the same outcome (to change the line colour to purple) but this requires different sets of instructions in logo (`SETPENCOLOR [# # #] -`) to scratch (set pen color to [selected color from menu] ). While this instructions are very similar they can only be interpreted by their relative programs. For this reason it is useful to get the children to first plan their program as an algorithm before translating it to the appropriate language.

### **Logical reasoning**

Logical reasoning is one of the 6 key concepts of computational thinking and is concerned with a systematic approach to solving problems or deducing information using a set of universally applicable and totally reliable rules. The use of our experiences and understanding of a topic or concept to help solve a problem or deduce information. When decoding words children use their knowledge of phonics to deduce how a word might sound. Upon seeing the word *cinder* for the first time, a child, applying logical reasoning, would predict that the word has a soft c sound because their experience of other *ci* words. Children are expected to use their knowledge of the software or hardware they are using to help solve problems and fix errors. A child who knows that a bee-bot has to travel the long way around rather than jumping over a gap, is showing and applying their knowledge. When creating an animation in scratch, a pupil will identify the need for delays when characters are in conversation. For pupils to be able to apply logical reasoning we must give them suitable opportunities to engage with purposeful problem solving.

### **Output**

The information produced by a computer system for its user, typically on a screen, through speakers or on a printer, but possibly through the control of lights, motors, etc. in physical systems.

### **Pattern recognition**

In many areas of the curriculum, we ask children to identify patterns. This might be the key features of a specific author's openings, what happens when two odd numbers are added or the most common shops on a high street. Once patterns have been identified, pupils are required to use these patterns to make predictions, create solutions and develop reasoning. When creating a quiz using scratch, a child may identify and fix a common problem with the scoring systems by resetting the variable value to zero at the start of the script. When moving on to creating more complex

games or using a different programming language, the child should readily identify the need to reset any variables to the initial value at the beginning of the program.

## Program

A program is an algorithm that is written in (or translated to) a language that a computer understands. The computer follows these instructions precisely and therefore they need to be unambiguous. When using Logo we might want the turtle to move up the screen but the command `up` is not one that the computer understands, so we have to use the predefined vocabulary and the correct syntax, in this case `FD 10`. Similarly when constructing a square, if we read an instruction telling us to turn right we would assume that we need to turn 90°. However a computer, a device with no intelligence, would not query this and would follow the instruction given.

## Repetition

When writing programs we should encourage children to be concise. Repetition is a way to get the computer to follow the same set of instructions forever, a given number of times or until a condition is met. When writing a program to create a square we can tell the computer to repeat the instruction `forward 10 right 90` four times. For most of us we repeat the same get up, eat breakfast, get ready, go to work algorithm each day until the day condition *is day Saturday or Sunday?* is met. Repetition is sometimes referred to as loops or forever loops and are often combined with selection statements.

## Search

To identify data that satisfies one or more conditions, such as web pages containing supplied keywords, or files on a computer with certain properties.

## Selection

Part of a computer program that is only executed if a certain condition is met. They share a lot in common with modal verbs and conditional sentences. It is useful to think of the words *if, then, else* when creating unplugged selection procedures. For example, when walking through a maze trying to avoid the *Great Fire of London* pupils might use the following selection statement: **If** there is fire in front of me **then** turn around **else** carry on. When creating programs we can use variables, internal and external inputs in selection statements. For example when using a class noise monitoring system, a warning sign may appear on screen when the noise level exceeds a given threshold.

## **Sequence**

When we create algorithms we must sequence the steps in the order they have to be followed. For example, when putting fuel in the car the fuel-tank cap has to be removed, then the nozzle inserted, before fuel is pumped into the car. If this set of instructions is sequenced in a different way we will not get the petrol into the fuel tank. Think of the puzzle whereby we need to get the farmer, the chicken, the fox and the corn across the river. If the steps are not sequenced correctly then either the corn, the chicken or both will get eaten. Pupils need to understand that digital devices follow programs blindly they will do what they have been instructed to do in the order given.

## **Services**

Programs running on computers, typically those connected to the internet, which provide functionality in response to requests; for example, to transmit a web page, deliver an email or allow a text, voice or video conversation.

## **Simulation**

Using a computer to model the state and behaviour of real-world (or imaginary) systems, including physical and social systems; an integral part of most computer games.

## **Software**

Computer programs, including both application software (such as office programs, web browsers, media editors and games) and the computer operating system. The term also applies to 'apps' running on mobile devices and to web-based services.

## **Variables**

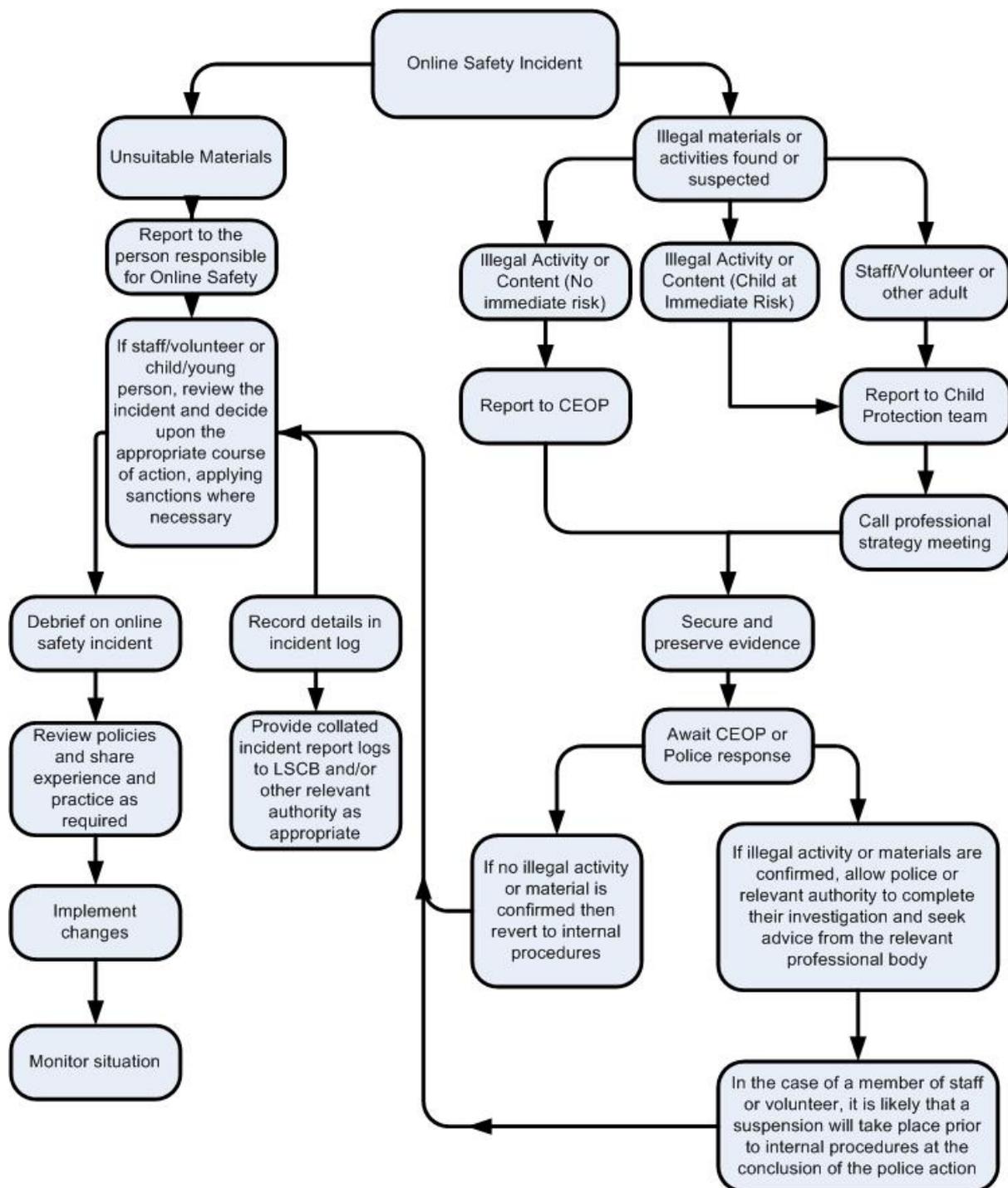
Variables are a way that computers can store, retrieve or change simple data. Children will experience variables when they play computer games: when certain tasks are completed the score will increase; if a character does something wrong a life maybe lost; a time limit may be set on completing a maze game. When marking a spelling test, children create a variable called score and they use the following instruction to change the variable: if spelling correct then increase score by one. This variable is stored and then changed after the next spelling. At the end of the test they can retrieve their score to give to the teacher.

## **World Wide Web**

A service provided by computers connected to the internet (web servers), in which pages of hypertext (web pages) are transmitted to users; the pages typically include links to other web pages and may be generated by programs automatically

Appendix 1:

# Responding to incidents of misuse – flow chart



Appendix 1 continued:

## Record of reviewing devices / internet sites (responding to incidents of misuse)

Date: .....

Reason for investigation: .....

.....  
.....  
.....

### Details of first reviewing person

Name: .....

Position: .....

Signature: .....

### Details of second reviewing person

Name: .....

Position: .....

Signature: .....

### Name and location of computer used for review (for web sites)

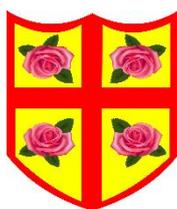
.....  
.....

Web site(s) address / device

Reason for concern

Web site(s) address / device	Reason for concern

### Conclusion and Action proposed or taken

## Appendix 2:

# Staff and Volunteer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the pupils in my care in the safe use of digital technology and embed online safety in my work with pupils.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these school technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses to communicate with on school matters.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in accordance with the school policy on Data Protection. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

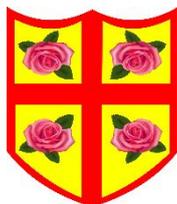
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

## Appendix 3:



# Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

## **Acceptable Use Agreement**

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:

Signed:

Date:

# Pupil Acceptable Use Agreement

## KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

# Pupil Acceptable Use Agreement

## KS2

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line at school.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet for research I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include: loss of access to the school network / internet, contact with parents/carers and in the event of illegal activities involvement of the police.

### **Pupil Acceptable Use Agreement Form**

If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines:

Name of Pupil: .....

Signed: .....

Date: .....

Parent / Carer Countersignature

Signed: .....

Date: .....

# Solgrid

The Solihull grid for learning



## Pupils and smart watches

Advice for schools

---

**Some schools have recently raised concerns about pupils wearing smart watches in schools.**

- The functionality of smart watches varies considerably: from being a fully-functioning smart phone (able to make phone calls, send texts, take photos, make videos and record conversations) to being solely a health monitor (recording the wearer's vital signs and activity). Although possible, it is difficult, and time-consuming, to distinguish between devices to understand the functionality of each device.
- Secondary schools, generally, have already had to address this issue and most secondary schools ban pupils from wearing all smart watches during the school day.
- **We believe the most significant safeguarding risk is from pupils having the ability to record themselves, other pupils and staff, which could even be done covertly.** There have even been examples of pupils recording other pupils and staff during school time and publishing the recordings on the internet.
- Some smart watches – even those that just monitor health – are expensive. We believe there is a strong likelihood that school staff would become embroiled in time-consuming incidents should pupils lose or damage smart watches during the school day. Condoning the wearing of smart watches at school could raise liability issues.
- **We believe that the safest and most effective response for schools is to tell parents that pupils are not allowed to wear smart watches during the school day for the same reasons that pupils are not allowed to use mobile phones during the school day.**
- **Schools should already have local arrangements in place, addressing the use of smart phones by pupils in school. We believe pupils' use of smart watches should simply be an extension and reflection of these arrangements – added to existing home/school agreements or pupil acceptable use policies.**

## Pupils and smart watches

### Examples of smart watches

*All taken from Amazon.co.uk to demonstrate the range and functionality of smart watches and how similar they can superficially appear.*

Supplier	<b>Youen</b>	
Cost	<b>£33</b>	
Connectivity	<b>SIM</b>	
Phone calls	<b>Yes</b>	
Camera	<b>Yes</b>	
Audio	<b>Yes</b>	
Social media	<b>Yes</b>	
Health monitor	<b>Yes</b>	
Comments	Functionally indistinguishable from a smart phone.	

Model	<b>Apple Watch (series 4)</b>	
Cost	<b>£499</b>	
Connectivity	<b>SIM</b>	
Phone	<b>Yes</b>	
Camera	<b>No</b>	
Audio	<b>Yes</b>	
Social media	<b>Yes</b>	
Health monitor	<b>Yes</b>	
Comments	Some only have connectivity to a iPhone but these have an identical appearance.	

Model	<b>Fitbit Versa</b>	
Cost	<b>£150</b>	
Connectivity	<b>Bluetooth</b>	
Phone	<b>When paired to phone</b>	
Camera	<b>No</b>	
Audio	<b>When paired to phone</b>	
Social media	<b>When paired to phone</b>	
Health monitor	<b>Yes</b>	
Comments	Linked smart phone provides wider functionality.	

## Supporting advice to parents

Outside school, some smart watches – such as health monitors – pose no appreciable risks to children. Other smart watches pose similar, even identical, risks to children as those posed by smart phones.

Parents and carers will have opinions about the use of mobile phones and smart watches in and out of school. And, obviously, what parents and carers do outside school is their own concern. However, schools might wish to refer parents to other sources of information.

- The negative behaviour impacts of the use of smart phones and other technologies in class has been highlighted in [Creating a Culture: how school leaders can optimise behaviour \[link\]](#), **Tom Bennett's** independent review of behaviour in schools commissioned by the Department for Education.
- The **Children's Commissioner** has recently issued *Who knows what about me?* The report looks at the use and collection of children's data, noting risks around the using of smart watches and data tracking. The report is available from [here \[link\]](#).
- Kent County Council has produced a [Guide to mobile web safety \[link\]](#) with Carphone Warehouse and Professor Tanya Byron, author of *The Byron Review: safer children in a digital world*.
- Simple internet searches (such as *smartwatch risks for children uk*) will gather relevant issues with internet safety.

## Curriculum links

The UKCCIS online safety curriculum framework [Education for a Connected World \[link\]](#) includes the use of smart phones and other devices. Smart watches are part of the changing landscape of technology available to children and should be included in online safety education.

### Getting help or more information

Name	<b>David Butt</b>
Email	<a href="mailto:dbutt@solihull.gov.uk">dbutt@solihull.gov.uk</a>
Telephone	<b>0121 704 6407</b>

Version control			
Version	Date	Owner	Notes
01b	12/01/19	DB	Initial version for schools following safeguarding subgroup (11/01/2019).

This document is consciously designed in black and white – to reduce printing costs.