



**Stonehouse Park**  
**Infant School**

The BEST start for every child so every  
can be the best they can be.

## **Policy for E Safety**

**Updated: February 2021**

**Ratified by Governors: February 2021**

**Review Date: February 2022**

## **Our Vision Statement**

**For every child to set out confidently on the adventure of learning: curious about the world, excited about their future, positive of their ability and caring towards other people.**

### **Our Aims:**

#### **Curious about the world**

- To promote awareness and understanding of other cultures.
- To develop the children's motivation, discovering their special interests and talents.
- To introduce children to a wide range of new experiences, ideas and activities.
- To encourage the children to ask questions about the world, talk about their ideas and express their opinions.

#### **Excited about their future**

- To make children excited about learning and eager to move on to the next stage of their learning.
- To help children to look beyond their immediate surroundings and their own personal circumstances.
- To shape a curriculum which will develop the knowledge and skills that children will need to meet the challenges of their future lives.
- To involve children in problem solving and develop their capacity to be active citizens

#### **Positive of their ability**

- To help children to reach the highest levels of achievement in all they do.
- To demonstrate to all children that they are able to learn and that they can succeed.
- To provide the highest quality of teaching for all children and to meet every child's individual needs.
- To develop children's awareness of their own learning and the value of resilience, perseverance and dedication.

#### **Caring of other people**

- To develop sensitivity to the feelings and concerns of other people.
- To demonstrate compassion, respect for others and develop a moral understanding.
- To learn how to co-operate and work with other people.

In line with our vision , The BEST Start For Every Child, the staff and governors at Stonehouse Park Infant School acknowledge the key role that information technology plays in the lives of our children and also the importance of being safe whilst engaging with technology.

This policy applies to all members of the school (including staff, children, volunteers, parents/carers, visitors and community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as reasonable to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviours. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviours and anti-bullying policies and will, where know, inform parents/carers of incidents of inappropriate e-safety behaviours that take place out of school.

## **2. Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities and individuals and groups within the school.

### **2.1 Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors received regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of E-Safety Governor. Their role will include:

- Regular meetings with the E-Safety Coordinator
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors/Board/committee/meeting (Learning and Achievement)

### **2.2 Head Teacher and Senior Leaders**

- The Head Teacher has a duty of care for ensuring the safety (including e-safety\_ of members of the school community.
- The Head Teacher and (at least) one member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head Teacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### **2.3 E-Safety Coordinator**

- Reports to the e-safety committee
- Takes day to day responsibility for the e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority/relevant body
- Liaises with the school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with E-Safety Governor to discuss current issues, reviews incident logs and filtering/change control logs
- Attends relevant meetings/committee of Governors
- Reports regularly to Senior Leadership Team

### **2.4 Technical Support Staff**

Technical support staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices
  - Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate
  - Any e-safety technical solutions such as internet filtering are operating correctly
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety Coordinator and Head Teacher
  - That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
  - That the use of network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher/Senior Leadership/E-Safety Coordinator

### **2.5 Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and the current school E-Safety Policy
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head teacher/E-Safety Coordinator for investigation/action/sanction
- All digital communications with children/parents should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspect of the curriculum and other activities
- Children understand and follow the E-Safety and Acceptable Use Policies'
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies in lessons and other school activities and implement current policies with regard to these devices
- In lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in places for dealing with any unsuitable material that is found in internet searches

## **2.6 Designated Safeguarding Leads:**

Should be trained in e-safety issues and aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Potential or actual incidents of grooming
- Cyber-bullying

## **2.7 Children**

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/using of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions of our school, if related to their membership of the school

## **2.8 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, websites and information about national/local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website
- Their children's personal devices in school (where this is allowed)

## **3. Policy Statements**

### **3.1 Education – children**

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety should be a focused in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum lesson should be provided as part of Computing/PSHE/other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Children should be taught in all lessons to be critically aware of materials/content they access online and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be helped to understand the need for the Pupil Acceptable Use Agreement and be encouraged to adopt a safe and responsible use both within and outside of school
- 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 children 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 children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites young people visit

- it is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, etc.) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, which clear reasons for the need.

### **3.2 Education – Parents/Carers**

Many parents and carers have only a limited understanding of e-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 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, websites
- Parents evenings
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications

### **3.3 Education and Training – Staff**

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

- A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety training as a training need within the performance management process.
- All new staff should receive e-safety training as a part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Coordinator will receive regular updated through attendance at external training events and by reviewing guidance documents released by relevant organisations
- The E-Safety Policy and its updates will be presented and discussed by staff in staff meetings/INSET days
- The E-Safety Coordinator will provide advice/guidance/training to individual as required

### **3.4 Training – Governors**

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

- Attendance at training provide by the Local Authority/National Governors Association or other relevant organisation

- Participation in school training/information sessions for staff

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

The school and Technical Support Staff (Robert Hall) will be responsible for ensuring that the school infrastructure/network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- 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
- The Head Teacher/LA Officer 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 children.
- 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 data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary "guest" (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

#### **5. Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying 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 policies to reduce the likelihood of the potential for harm.

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

particular they should recognise the risk attached to publishing their own images on the internet e.g. on social networking sites

- In accordance with guidance from the Information Commissioner's Office, parents/carer are welcome to take videos and digital images of their own children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not include other children nor be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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 children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, social networking site or elsewhere that include children will be selected carefully and comply with good practice guidance on the use of such images
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents/carers will be obtained at the beginning of the academic year/upon joining the school before photographs of their children are published on the internet

## **6. Data Protection**

**6.1** Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

## **6.2** The school must ensure that:

- 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 purpose it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained on accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a data protection policy
- It is registered as a Data Controller for the purposes of the Data Protection Act
- Responsible persons are appointed/identified – Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensures that such data storage meets the requirements laid down by the Information Commissioner's Office.

## **6.3** Staff must ensure that they

- 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

## **7. Communications**

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

Communication Technologies	Staff/Other Adults				Pupils				
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought into school		✓						✓	
Use of mobile phones in lessons	✓				✓				
Use of mobile phone in social times		✓			✓				
Taking photos on mobile phone/cameras			✓					✓	
Use of other mobile devices e.g. tablets, gaming devices			✓					✓	
Use of personal email addresses in school, or on school network			✓		✓				
Use of school email for personal emails	✓				✓				
Use of messaging apps			✓		✓				
Use of school social media				✓					
Use of personal social media			✓		✓				

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

- The official school email service may be regarded as safe and secure. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others about school matters.
- Users must immediately report any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and children or parents/carers must be professional in tone and context. These communications may only take place on official (monitored) school email accounts. Personal email addresses, text messaging or social media must not be used for these communications
- Children should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website or social media sites. Only official email addresses should be used to identify members of staff.

## **8. Social Media – Protecting Professional Identity**

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to children, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the E-Safety Coordinator to ensure compliance with the Social Media Policy.

## 9. Unsuitable/Inappropriate 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 school or outside school when using school equipment or systems. The school restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</b>	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	
	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				X		

safeguards employed by the school / academy					
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. 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)					
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			

## 10. Responding to Incidents of Misuse

**10. 1** This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above – subsection 9).

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 the 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 children 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 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)
- 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
  - Police involvements 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:
  - Incident of 'grooming' behaviour
  - The sending of obscene materials to a child
  - Adult material which potentially breaches the Obscene Publications Act
  - Criminally racist material
  - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## **10.2 School Actions and 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 as follows:

Staff								
Incidents	Refer to E-Safety Coordinator	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school's network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules	X	X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X				X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X					X
Actions which could compromise the staff member's professional standing	X	X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X					

Deliberately accessing or trying to access offensive or pornographic material	X			X			X	
Breaching copyright or licensing regulations	X	X						X
Continued infringements of the above, following previous warnings or sanctions	X	X					X	X

Children									
Incidents	Refer to class teacher	Refer to E-Safety Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X			
Unauthorised use of social media / messaging apps / personal email		X				X		X	
Unauthorised downloading or uploading of files	X	X			X				
Allowing others to access school network by sharing username and passwords	X	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X							
Attempting to access or accessing the school network, using the account of a member of staff		X	X			X			X
Corrupting or destroying the data of other users		X			X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X			X
Continued infringements of the above, following previous warnings or sanctions		X	X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system		X				X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X		X	X

Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X						X

February 2021