STAVERTON
CHURCH OF ENGLAND
PRIMARY SCHOOL

Staverton C of E Primary School
Online safety Policy 2021-2022

Introduction

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is 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 behaviour. This is pertinent to incidents of cyber-bullying or other Online 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 behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school. Online safety is part of our whole school safeguarding approach.

This policy should be read and understood in conjunction with the following documents:

- Behaviour Policy 2021
- Anti-Bulling Policy 2021
- Child Protection Policy 2021
- Guidance for Safer Working Practice for Adults working with Children and Young People
- Keeping Children Safe in Education 2021
- Screening, Searching and Confiscation at schools (DfE 2016)
- Social Networking Policy (WSCB)
- Staff Code of Conduct 2021 update
- Staff Behaviour Policy 2021
- Personal use of Social Media by teachers and support staff policy 2021

Aims

Our aim is to provide pupils and staff with the knowledge, skills and confidence to become safe and responsible users of technology.

Roles and Responsibilities

Governors

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- The Governors will receive regular information about Online Safety incidents and monitoring report.
- The role of the Online Safety Governor should include regular attendance at Online Safety Group meetings, regular monitoring of filtering and online safety incident logs and regular meetings with the Online Safety Co-Ordinator.

Headteacher (Mr E Powe)

- The Head Teacher is responsible for ensuring the safety (including Online Safety) of members of the school community, although the day to day responsibilities will be delegated to the Online Safety Co-ordinator.
- The Head Teacher is responsible for ensuring that the Online Safety Co-ordinator receives suitable CPD to enable them to carry out their role and to train other colleagues, as relevant.
- The Head Teacher and another member of the Senior Leadership Team should be made aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online Safety Co-ordinator (Miss L Smith)

- 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 with support from the Senior Leadership Team
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of Governors
- Reports to Senior Leadership Team

Teaching and Support Staff

- Staff should have an up to date awareness of Online Safety matters and of the current school policy and practices.
- Staff should ensure they have read, understood and signed the Staff Acceptable Use Agreement.
- Staff should report any misuse or problem to the Headteacher / Online Safety Lead /DSL for investigation
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Staff must be aware of Online Safety issues related to mobile phones, cameras and hand held devices (such as iPads), as well as PC's.

- Staff must exercise caution when visiting non-filtered sites (such as You Tube). Staff should check these websites before sharing with children, and ensure their browser is closed when not in use.
- Staff should maintain and apply a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism (for more information, please refer to the Child Protection Policy).
- Staff should only use school software for the purpose of classroom use. Photos of children should be taken only on class iPads. Only in exceptional circumstances should they use personal digital devices (such as mobile phones, personal cameras etc). If this situation arises, the Head Teacher must be informed.
- Staff should be aware that Internet traffic is monitored and reported by the SWGfl and can be traced to the individual user. Discretion and professional conduct is essential.
- The school's consequences for Internet and mobile phone/PDA/technology misuse will be clear so that all teachers are confident to apply this should the situation arise.

Technical Staff (Soft Egg)

The school's managed ICT Service is provided by an outside contractor; however it remains the responsibility of the school to ensure that the appointed contractor carries out all the required online safety measures and is fully aware of the school's policy. These include ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required online safety technical requirements and any external (i.e. DfE/Local Authority guidance that may apply)
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis by SWGfL and that the implementation is not the sole responsibility of any single person
- 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher for investigation and any subsequent action that might be required
- That monitoring software systems are implemented and updated as agreed in the school's policy

Pupils

- Pupils are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school
- Pupils should know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. If staff or pupils discover unsuitable sites, this should be reported to the Online Safety Co-ordinator and reported to the Headteacher. The URL (address) and content must be reported to the South West Grid for Learning: 0845 307 7870 or email: abuse@swgfl.org.uk
- Pupils should understand school policies on the taking/use of images and on cyber bullying. They should realise that the school's Online Safety Policy also covers their actions out of school, if related to a member of staff of fellow pupil. (Directed Online Safety sessions will take place annually to raise

awareness of this). Rules for Internet access will be posted in all rooms where computers and iPads are used.

- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- The use of online chat or access to social networking sites is not permitted in school, other than as part of any online learning environment.
- When using digital images, pupils should be aware 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 (e.g. on social networking sites).
- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Where pupils in KS2 are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. 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 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.

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

- Parents/Carers should endorse the Pupil Acceptable Use Agreement.
- Parents/Carers will have access to the Online Safety Policy/Pupil Acceptable User Agreement via the school website. They will also be informed on any Online Safety initiatives (such as Online Safety Fortnight) via the website, newsletters, Parents' Evenings etc.
- Parents/Carers should liaise with the school with regards to any Online Safety concerns or potential risks.
- Interested parents will be referred to organisations such as Childnet International, PIN, Parents Online and NCH Action for Children. Further to this, an Online Safety conference for parents will be run by the NSPCC.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Designated Safeguarding Lead (DSL):

The DSL should be trained in Online Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

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

Concerns regarding the online safety of pupils should be reported to the DSL or DDSL immediately and recorded on CPOMS.

Authorised Access

'*Children have unlimited and unrestricted access to the internet via mobile phone networks'* Keeping Children Safe in Education, 2021.

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. At Staverton we are aware that children have unlimited access to the internet. We ensure that children at taught about the potential dangers of the internet.

- Staverton CE Primary School receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.
- Teachers have access to unfiltered internet. They need to request a login from Soft Egg our ICT technicians. When they have finished they need to ensure that they have logged out.
- Our home-school agreement includes the Responsible Use Policy and guidance for sound, image and video for web publication. (See The Wiltshire E Safety Toolkit).
- Staverton School's Internet access will be designed expressly for children's use and will include filtering appropriate to the age of the children.
- In the Early Years' Foundation Stage, access to the internet is likely to be by adult demonstration only. In Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- At Key Stage 2, children will be able to search the internet independently, using child-friendly, approved search engines, with the children being taught appropriate keywords with which to search. The children will be supervised at all times. Children will be taught what to do if they come across unsuitable and inappropriate materials so that these skills are embedded by the time they are using the internet independently.

Technical – infrastructure/equipment, filtering and monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupils to staff. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed or any consequence of the internet access.

- A log of all staff with unfiltered access to the internet will be kept and regularly reviewed
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- SWGfL regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

- An appropriate system is in place for users to report any actual or potential technical incident and/or security breach to the relevant person, as agreed.
- Pupils will be made aware of the importance of filtering systems through the online safety education programme and will also be warned of the consequences of attempting to subvert the filtering system.
- Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the ISP via the Online Safety Coordinator.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head Teacher, LADO, Police, Internet Watch Foundation.
- The use of computer systems without permission or for inappropriate purposes could constitute and office under The Computer Misuse Act 1990

Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Teaching and Learning

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

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

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced regularly
- 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 pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside 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 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 the young people visit.
- All video clips shown in class must have been watched prior to being shown and checked for appropriate content.
- No content that is rated above the age of the pupils watching may be accessed or shown to children. No content rated 12+ may be shown in school.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (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 auditable, 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 online 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, web site
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education & Training – Staff

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- 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 Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in Professional Development meetings.
- The Online Safety Lead (or other nominated person) 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 group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

Communication and Content

Website Content

Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs or videos of pupils are published on the school website/blog. Photographs/ videos will be selected carefully and will not enable individuals to be clearly identified.
- Pupils' names (first and/or surname) will not be used in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Schools will need to determine the best approach for their circumstances, based upon pupil age and curriculum requirements. Pupils will only use their class email address (classname@staverton.wilts.sch.uk) when sending emails and responses should be viewed by the teacher to check appropriateness before being read by the pupils.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a responsible adult if they receive offensive e-mail.
- Staff will use official school provided email accounts.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is banned.
- Any document attachments which pertain to children must be encrypted before sending.
- Any portable devices that are linked to school email laptop/IPADs must be password protected.

Remote Learning

During periods of partial school closure i.e. during a national lockdown, the school will provide remote learning. This will be delivered via Google Classroom. All pupils will be provided with a unique username and password. This will be administered by the school's IT technicians. The learning platform is secure and is only for use by Staverton pupils and parents. Pupils and their parents will be able to access daily learning opportunities as well as turn in work to be marked and message their teachers. Senior school leaders will be members of every Google Classroom class. Materials posted to Google Classroom will include printable resources, pre-recorded lessons and editable documents. 'Live' opportunities such as assemblies, lessons and learning support will also be available to children. These sessions will be offered through Google Meet which is accessed via secure, unique usernames and passwords. All Google Meet sessions will be recorded by Staverton staff. The individual email function in Google Classroom has been switched off for pupil accounts.

Loaning of school devices

There may be times when the school will loan a school owned device to children to use for example during a national lockdown. Where this is needed the device will be checked by the IT technicians before being loaned and will be checked again on return to school. Parents/carers will sign a loan agreement prior to taking the device home.

Mobile Technology

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet access all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly and that they do not impede teaching and learning. Staff will be given clear boundaries on professional use.

The use of mobile phones and personal devices is a school decision, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Children and staff have access to resources to support learning and teaching
- Our school community will be given clear boundaries on responsible and professional use
- These principles underpin our policy, which states that:
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community

Policy for children

- Mobile phones that are brought in to school by children will be stored in the School Office during the school day. However, they remain the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.
- Children must not take mobile phones on school trips or residential visits unless agreed by the head teacher for medical reasons e.g. diabetes
- School staff authorised by the Head teacher may search children or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.

Policy for staff and visitors

- Mobile phones that are brought into school by any member of staff or visitors must be stored remotely, away from the classrooms. Lockers are available for this purpose or they may be stored in the School Office during the school day. However, the school accepts no responsibility for the loss, theft or damage of such items.

- Staff mobiles will be turned off during teaching time, non- contact time and turned to silent during any staff or school led meeting.
- Personal electronic devices provided by the school may be used during lessons or formal school time as part of approved and directed curriculum-based activity.
- Where staff may need to contact children and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail or phone), unless under the direction of the headteacher e.g. residentials. In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- During school hours, where family members may need to contact staff in an emergency situation, they should telephone the School Office in the first instance. Only in exceptional circumstances, and in agreement with the Head Teacher, will a member of staff be allowed to use a mobile phone during learning time.
- Staff will be provided with school equipment for the taking of photos or videos of children for educational purposes and will only use work-provided equipment for this purpose.
- Wherever possible, contractors will be asked to carry out maintenance outside of school hours. Where essential maintenance or emergency repair is required in teaching areas during school hours, all contractors will be supervised to comply with this policy.
- For the safeguarding of all involved, users must connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user’s device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy
- A school mobile phone will be passcode protected and given to the designated Trip Leader to ensure confidentiality of mobile records.

Video Conferencing

- Video conferencing (including FaceTime, Google Classrooms, Skype, Teams and Zoom) enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many potential benefits in education and where possible should take place using the school’s wireless system.
- Staff must refer to the internet consent agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised by the class teacher at all times when involved in video conferencing.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-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 students/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 e.g. on social networking sites.
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites.
- 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 students/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 students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Communications:

- The official school email service may be regarded as safe and secure and is monitored. All users should be aware that email communications are monitored.
- Users must immediately report to the nominated person, in accordance with the school‘s 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 communications.
- Any digital communication between staff and pupils or their parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. (For further information please refer to the school's Social Networking Policy

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
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).

- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- It provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

- When personal data is stored on any mobile device or removable media the:
  - data must be encrypted and password protected.
  - device must be password protected.
  - device must be protected by up to date virus and malware checking software
  - data must be securely deleted from the device, in line with school policy (below) once it has been

- transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT 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:

- Ensuring that personal information is not published
- Training is provided including: 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 students/pupils, 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

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.
- Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to school social media sites e.g. twitter, Facebook

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly to ensure compliance with the school policies.

Cyber Bullying

Many children and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that children, school staff and parents/carers understand how cyber-bullying is different from other forms of bullying. It is important to understand how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety within our school.

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007. Examples of how cyberbullying may occur include via mobile phones, social networking sites, gaming, forums, email and sexting. The DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: http://www.digizen.org/cyberbullying. Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies.
Cyber-bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Anti-bullying and Child Protection policies, which include:

- Clear procedures are in place to investigate incidents or allegations of cyber bullying.
- Clear procedures are in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded and investigated by the designated Safeguarding Lead.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Children, staff and parents/carers will be required to work with the school.

Handling of complaints

- Any complaint about staff misuse must be referred to the Head Teacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling.
  - informing parents or carers.
  - removal of Internet or school technology access for a period, which could ultimately prevent access to files held on the system.

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 technicians may, at times, need to test access to ensure firewalls and safeguards are in place. Where this occurs lists of inappropriate sites will be updated and blocked.

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:

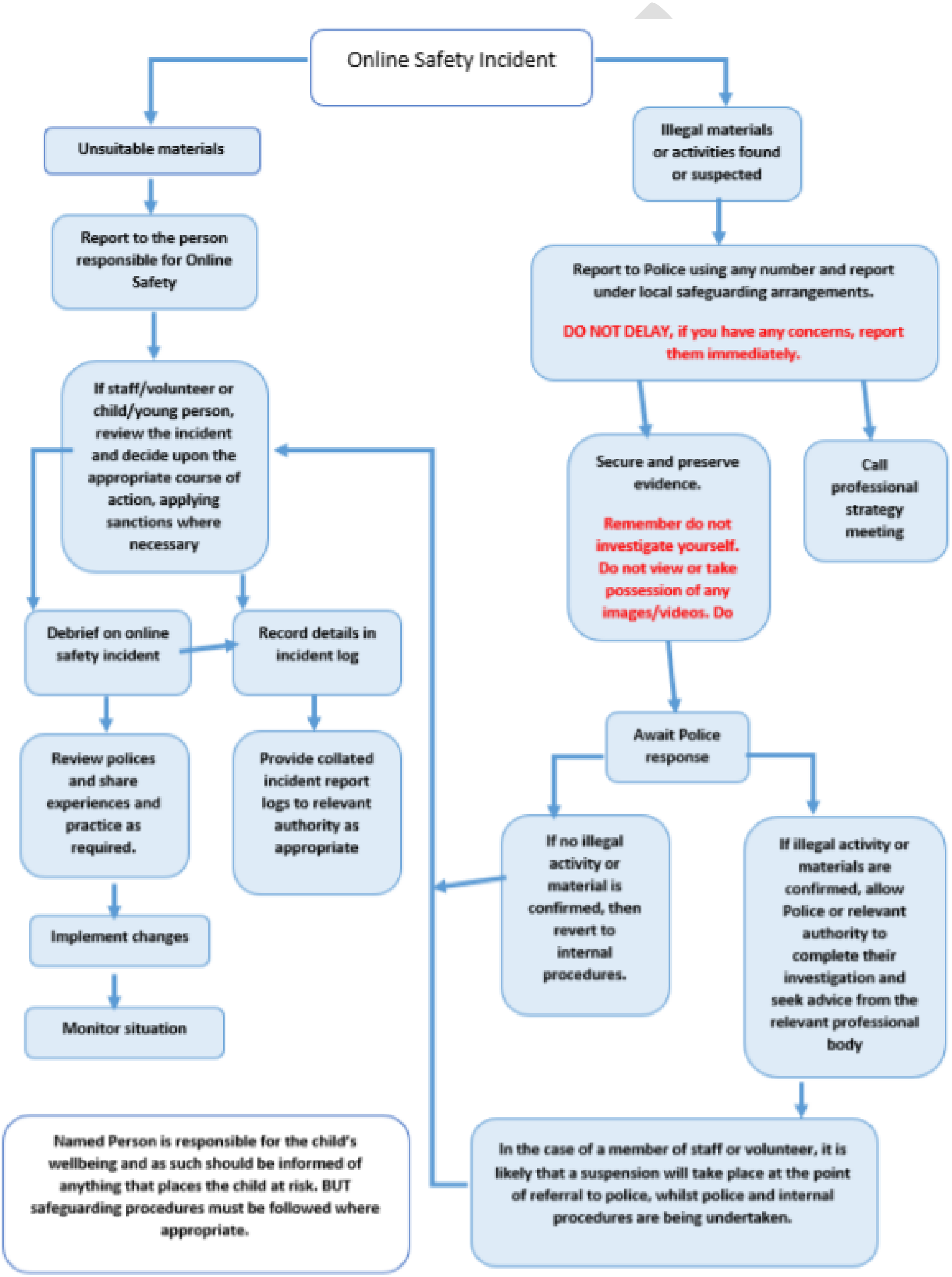
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					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 “User Actions” above).

Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Named Person is responsible for the child’s wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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

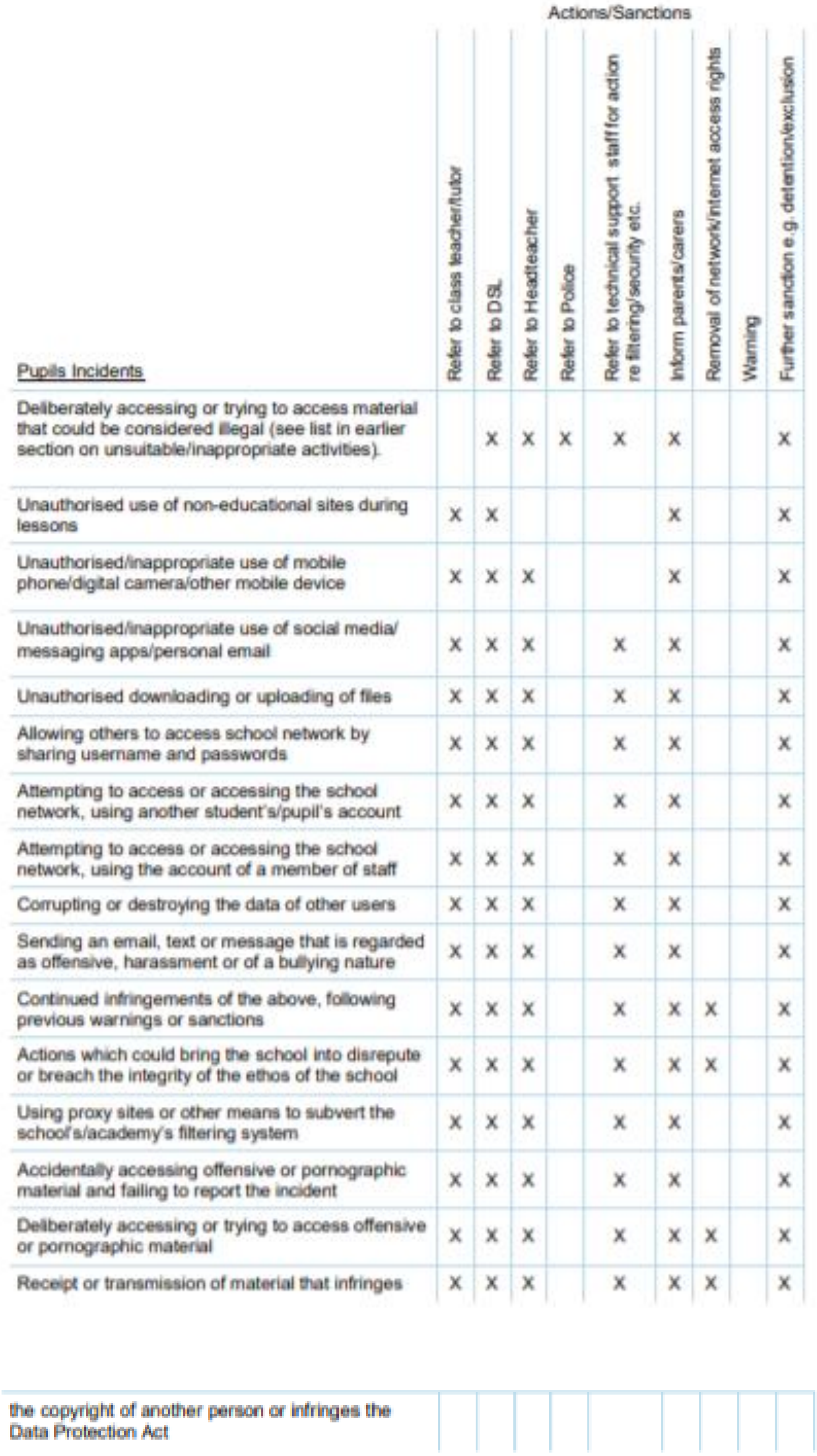
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act (see User Actions chart above)
  - 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 as follows**:**



	Actions/Sanctions								
Pupils Incidents	Refer to class teacher/tutor	Refer to DSL	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
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	X			X
Unauthorised use of non-educational sites during lessons	X	X				X			X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X			X			X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X		X	X			X
Unauthorised downloading or uploading of files	X	X	X		X	X			X
Allowing others to access school network by sharing username and passwords	X	X	X		X	X			X
Attempting to access or accessing the school network, using another student's/pupil's account	X	X	X		X	X			X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X			X
Corrupting or destroying the data of other users	X	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			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		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	X	X		X
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X	X		X	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	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		X	X	X		X

	Actions/Sanctions							
Staff Incidents	Refer to DSL/LADO	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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	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		X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X	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			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	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		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			X
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X			X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X	X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Appendices

Wiltshire
COUNTY COUNCIL

STAVERTON
CHURCH OF ENGLAND
PRIMARY SCHOOL

202 Rules for Responsible Internet and Device Use for Adults

I will use all ICT equipment issued to me in an appropriate way, in line with the Online Safety policy.

I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the owner's permission.
- Place inappropriate material, or that which may impact negatively on the School community, onto the Internet.
- Send e-mails that are offensive or otherwise inappropriate.
- Disregard my responsibilities for security and confidentiality with regard to children's identities and data protection. Download files that will adversely affect the security of the laptop/IPAD and school network.
- Update web pages or use pictures or text that can identify the school and individual children.
- Attempt to repair or interfere with the components, software or peripherals of any IT equipment that is the property of Staverton C E Primary School.
- I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
- When emails relate to children within the school, I will encrypt any attachments sent and ensure that only initials are used for identification.
- Any removable media I use will be encrypted and free from any type of virus.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Online Safety Lead or IT technician.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
- I will report immediately to the Headteacher or Online Safety Lead any unpleasant material or messages sent to me.
- I understand that consequences will be taken if I deliberately access Internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.
- I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop/IPAD removed and that other disciplinary consequences may follow.
- I agree to follow the Online Safety, in relation to the recreational use of social networking sites or other online technologies.
- My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
- I will ensure I keep my network password secure and inform the Office Manager if this security is breached.

Signed: .... Date: ....

STAVERTON
CHURCH OF ENGLAND
PRIMARY SCHOOL

Wiltshire
COUNTY COUNCIL

Rules for Responsible Internet Use for Children

These rules help us to be fair, responsible and keep everyone safe.

- I will ask permission before using the Internet and will only use the internet if there is an adult close by to supervise me.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school or use software or files from home.
- I understand that any mobile devices that I bring into school will be stored in the School Office.
- I will only e-mail and open attachments from people I know, or my teacher has approved, through the school system.
- Any messages I send will be polite and sensible.
- I understand that I must never post my home address, phone number or email address online, or arrange to meet someone.
- I will not use the Internet in school to access social media sites.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit and there may be consequences if anything inappropriate is found.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers and that my parents/carers may be informed.

I have read and understand the school rules for responsible internet use. I will use the computer system and internet in a responsible way and follow these rules at all times

STAVERTON
CHURCH OF ENGLAND
PRIMARY SCHOOL

Wiltshire
COUNTY COUNCIL

Staverton CE Primary School

Sample Letter to Parents

1st September 2021

Dear Parents

Responsible Internet Use

As part of your child’s curriculum and the development of ICT skills, Staverton CE Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, the South West Grid for Learning (SWGfL) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child’s use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

Staff Professional Conduct Agreement Laptop/IPAD policy for Staverton School staff

STAVERTON
CHURCH OF ENGLAND
PRIMARY SCHOOL

Wiltshire
COUNTY COUNCIL

- The laptop/IPAD remains the property of Staverton School.
- The laptop/IPAD is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Staverton School Staff should use the laptop/IPAD.
- On the teacher leaving the school's employment, the laptop/IPAD must be returned to Staverton School on the last day of the term in which they leave. Staff on extended leave of 4 weeks and over should return their laptop/IPADs to the school (other than by prior agreement with the Headteacher).
- When in school and not being used, the laptop/IPAD must be kept in a safe place. It must not be left in an unlocked, unattended classroom.
- Laptops and IPADs must not be left in an unattended car, due to the confidential nature of the data. In exceptional circumstances, if there is a need to do so, it should be locked in the boot.
- The laptop/IPAD must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher, with evidence of adequate insurance.
- All software on laptops and IPADS must be fully licensed and have been installed by our IT technician, to ensure that no corrupt software or systems are installed.
- If any removable media is used, then it must be encrypted and checked to ensure it is free from any viruses.
- It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop/IPAD is kept up-to-date.
- Staff must use their laptop/IPAD in school on the network at least once a week to ensure virus protection is automatically updated.
- Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
- Staff should communicate with the School's IT technician with regard to technical issues, or the need to modify the laptops/IPADs.
- Students can only use the laptop/IPAD under the direct supervision of an adult.
- If any fault occurs with the laptop/IPAD, it should be referred immediately to the IT Technician.
- The laptop/IPAD would be covered by normal household insurance. If not it should be kept in school and locked up overnight.
- The purchase and installation of Apps on school IPADS must be agreed by Computing Coordinator and carried out by appropriately authorised members of staff (IT Technician).

The device I have is ……………………………………………….. (Serial no. ………).

The device I have is ……………………………………………….. (Serial no. ………).

I agree to adhere to this Conduct Agreement. Signed: ………………………………….. Date: ……………………………….

Web-based Resources

For Schools

KidSmart http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org/
Guidance for parents, schools and pupils

London Grid for Learning
http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice
http://www.dfes.gov.uk/bullying/

Internet Watch Foundation
www.iwf.org.uk
Invites users to report illegal Websites

South West Grid for Learning – Safe
www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

For Parents

Kids Smart
http://www.kidsmart.org.uk/parents/
A Parent's guide to Internet devices

Childnet International http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

E-safety page on School website http://www.staverton.wilts.sch.uk/e-safety-1/

Useful contact details: South West Grid for Learning (SWGfL)

Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: 0870 9081708

E-mail: support@swgfl.org.uk

To notify of an inappropriate website: abuse@swgfl.org.uk