Styal Primary School

On-Line Safety Policy

Written September 2021

To be reviewed September 2022

## Development / Monitoring / Review of this Policy

4

This online safety policy has been developed by:

* Headteacher and senior leaders
* Online Safety Lead
* Staff – including teachers, support staff, technical staff
* Governors
* Parents and carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

The school will monitor the impact of the policy using: *(delete/add as relevant)*

* Logs of reported incidents
* Monitoring logs of internet activity (including sites visited)/filtering
* Internal monitoring data for network activity
* Surveys/questionnaires of
  + students/pupils
  + parents/carers
  + staff

Scope of the Policy

This policy applies to all members of the *Styal School* community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology 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 students/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 online-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 (see appendix for template policy). 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.

Roles and Responsibilities

7

Governors

*Governors* are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*. The role of the Online Safety *Governor* will include:

* regular meetings with the Online Safety Lead
* attendance at Online Safety meetings
* regular monitoring of online safety incident logs
* regular monitoring of filtering/change control logs
* reporting to relevant Governors

Headteacher and Senior Leaders

* The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Lead*. At Styal, this is the Headteacher.
* The Headteacher, Deputy Headteacher and DDSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority/MAT/other relevant body* disciplinary procedures). Online Safety BOOST includes an ‘Incident Response Tool’ that outlines the steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. More information is available at: <https://boost.swgfl.org.uk/>
* *The Headteacher and Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.* Online Safety BOOST includes access to unlimited online webinar training – further details are at <https://boost.swgfl.org.uk/>
* *The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
* *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead

* 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
* liaises with school technical staff
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
* meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering/change control logs
* attends relevant meetings of *Governors*
* reports regularly to Senior Leadership Team

Technical Staff

Those with technical responsibilities are responsible for ensuring:

* **that the *school’s* technical infrastructure is secure and is not open to misuse or malicious attack**
* **that the *school* meets required online safety technical requirements and any *Local Authority* online safety policy/guidance that may apply.**
* **that users may only access the networks and devices through a properly enforced password protection policy**
* *the filtering policy is applied and updated on a regular basis and that its 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 *networks/internet/digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Headteacher and Senior Leaders; Online Safety Lead* for investigation/action/sanction
* *that monitoring software/systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

Are responsible for ensuring that:

* **they have an up to date awareness of online safety matters and of the current *school* online safety policy and practices**
* **they have read, understood and signed the staff acceptable use policy/agreement**
* **they report any suspected misuse or problem to the *Headteacher /Online Safety Lead* for investigation/action/sanction**
* **all digital communications with students/pupils/parents/carers should be on a professional level *and only carried out using official school systems***
* online safety issues are embedded in all aspects of the curriculum and other activities
* students/pupils understand and follow the Online Safety Policy and acceptable use policies
* they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
* *in lessons where internet use is pre-planned students/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*

Designated Safeguarding Lead

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

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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governing Body.*

* the production/review/monitoring of the school online safety policy/documents.
* *the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.*
* mapping andreviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
* monitoring network/internet/filtering/incident logs
* consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
* monitoring improvement actions identified through use of the 360-degree safe self-review tool

Students/Pupils:

* **are responsible for using the *school* digital technology systems in accordance with the student/pupil acceptable use agreement**
* 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/use of images and on online-bullying.
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school’s* online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

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

* digital and video images taken at school events
* *their children’s personal devices in the school*

## Policy Statements

### Education – Students/Pupils

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 as part of a planned programme of assemblies and pastoral activities**
* **Students/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.**
* **Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
* **Students/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.**
* *Students/pupils should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.*
* *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 students/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 students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
* *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/academy will therefore seek to provide information and awareness to parents and carers through:

* *Curriculum activities*
* *Letters, newsletters, web site*
* *Parents/carers evenings*
* *High profile events/campaigns e.g. Safer Internet Day*
* *Reference to the relevant web sites/publications e.g.* [swgfl.org.uk](http://swgfl.org.uk)*,* [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)*,* <http://www.childnet.com/parents-and-carers>

### Education & Training – Staff/Volunteers

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

* **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**. Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff (<https://boost.swgfl.org.uk/>)
* **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.**
* *It is expected that some staff will identify online safety as a training need within the performance management process.*
* *The Online Safety Lead will receive regular updates through attendance at external training events by reviewing guidance documents released by relevant organisations.*
* *This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.*
* *The Online Safety Lead will provide advice/guidance/training to individuals as required.*

### Training – Governors

**Governors should take part in online safety training/awareness sessions**, with particular importance for those who are members of any 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/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
* Participation in school/academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

### Technical – infrastructure/equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online 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.**
* **All users will be provided with a username and secure password.****Users are responsible for the security of their username and password**.
* The “master/administrator” passwords for the school systems, used by the Network Manager must also be available to the *Headteacher* and kept in a secure place
* (Insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
* **Internet access is filtered for all users.** Illegal content (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/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
* *The school has provided enhanced/differentiated user-level filtering eg..staff / pupils.*
* *School technical staff 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/potential technical incident/security breach to the relevant person, as agreed.*
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
* An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
* *An agreed policy is in place* *that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.*

*An agreed policy is in place* *regarding the use of removable media (e.g. memory sticks) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured****.*

### Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

* **The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
* **The school allows:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | School Devices | | | Personal Devices | | |
|  | **School owned for single user** | **School owned for multiple users** | **Authorised device[[1]](#footnote-1)** | **Student owned** | **Staff owned** | **Visitor owned** |
| Allowed in school | *Yes* | *Yes* | *Yes* | *Yes/No**[[2]](#footnote-2)* | *Yes/No2* | *Yes/No2* |
| Full network access | *Yes* | *Yes* | *Yes* |  |  |  |
| Internet  only |  |  |  |  |  |  |
| No network access |  |  |  |  |  |  |

#### Personal devices:

* Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
* Restrictions on where, when and how they may be used in school
* Storage
* Whether staff will be allowed to use personal devices for school business
* Levels of access to networks/internet (as above)
* Network/broadband capacity
* Technical support (this may be a clear statement that no technical support is available)
* Filtering of the internet connection to these devices
* Data Protection
* The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
* Taking/storage/use of images

### 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.**
* **Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press.**
* In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school/academy 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, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
* Staff and volunteers are allowed to take digital/video images to support educational aims, 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/academy into disrepute.
* Students/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.
* Students’/Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Student’s/Pupil’s work can only be published with the permission of the student/pupil and parents or carers.

### Data Protection

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

#### The school must ensure that:

* **it has a Data Protection Policy.**
* **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
* **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.**
* **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**
* **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 and volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice**
* **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**](https://ico.org.uk/for-organisations/report-a-breach/) **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**

16

* **data must be securely deleted from the device, in line with school policy 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**

## 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 benefit of using these technologies for education outweighs their risks/disadvantages:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Staff & other adults | | | Students/Pupils | | | | | |
| Communication Technologies | 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 to the school/academy |  |  |  |  | |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  | |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  | |  |  |  |  |
| Taking photos on mobile phones/cameras |  |  |  |  | |  |  |  |  |
| Use of other mobile devices e.g. tablets, gaming devices |  |  |  |  | |  |  |  |  |
| Use of personal email addresses in school/academy, or on school/academy network |  |  |  |  | |  |  |  |  |
| Use of school/academy email for personal emails |  |  |  |  | |  |  |  |  |
| Use of messaging apps |  |  |  |  | |  |  |  |  |
| Use of social media |  |  |  |  | |  |  |  |  |
| Use of blogs |  |  |  |  | |  |  |  |  |

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

* **The official *school* email service may be regarded as safe and secure and is monitored.Users should be aware that email communications are monitored.**
* **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
* **Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
* *Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
* *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

### 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 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*
* *A code of behaviour for users of the accounts*
* *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.
* 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 private social media sites*

#### 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 by the Online Safety Group to ensure compliance with the school policies.

## Dealing with unsuitable/inappropriate activities

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

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

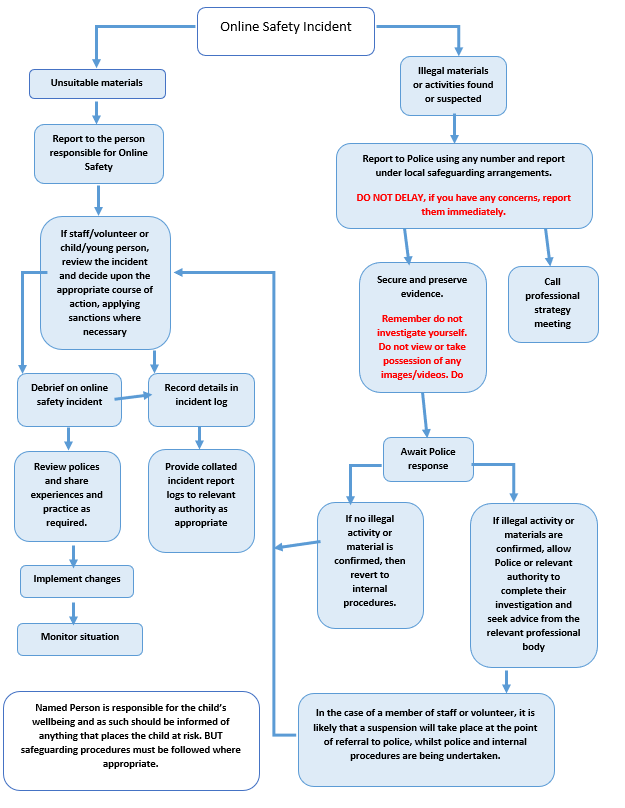
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User Actions  18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate 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](https://swgfl.org.uk/assets/documents/managing-sexting-incidents.pdf?_=1554476329) and [UKCIS – Sexting in schools and colleges](https://www.gov.uk/government/publications/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)   N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information [here](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved) | |  |  |  |  | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy | |  |  |  | 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) | |  |  |  |  |  |
| On-line gaming (non-educational) | |  |  |  |  |  |
| On-line gambling | |  |  |  |  |  |
| On-line shopping/commerce | |  |  |  |  |  |
| File sharing | |  |  |  |  |  |
| Use of social media | |  |  |  |  |  |
| Use of messaging apps | |  |  |  |  |  |
| Use of video broadcasting e.g. Youtube  19 | |  |  |  |  |  |

## 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.**



## 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** | | | | | | | | | | | | | | | | | | | |
| Students/Pupils Incidents | Refer to class teacher/tutor | | | Refer to Head of Department/Year/other | | Refer to Headteacher/Principal | | 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 | |  | |  | |  | |  | |  | | |
| Unauthorised use of non-educational sites during lessons |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Unauthorised/inappropriate use of social media/ messaging apps/personal email |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Unauthorised downloading or uploading of files |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Allowing others to access school/academy network by sharing username and passwords |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Attempting to access or accessing the school/academy network, using another student’s/pupil’s account |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Attempting to access or accessing the school/academy network, using the account of a member of staff |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Corrupting or destroying the data of other users |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Continued infringements of the above, following previous warnings or sanctions |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Using proxy sites or other means to subvert the school’s/academy’s filtering system |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Deliberately accessing or trying to access offensive or pornographic material |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 |  | | |  | |  | |  | |  | |  | |  | |  | |  | | |
|  | | | | **Actions/Sanctions** | | | | | | | | | | | | | | | | |
| Staff Incidents | | | Refer to line manager | | | Refer to Headteacher Principal | | 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 | |  | |  | |  | |  | |
| Inappropriate personal use of the internet/social media/personal email | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Unauthorised downloading or uploading of files | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| 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 | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Deliberate actions to breach data protection or network security rules | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Actions which could compromise the staff member’s professional standing | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Using proxy sites or other means to subvert the school’s/academy’s filtering system | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Deliberately accessing or trying to access offensive or pornographic material | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Breaching copyright or licensing regulations | | |  | | |  | |  | |  | |  | |  | |  | |  | |
| Continued infringements of the above, following previous warnings or sanctions | | |  | | |  | |  | |  | |  | |  | |  | |  | |

22

Appendix A

## Staff (and Volunteer) Acceptable Use Policy Agreement Template

### School Policy

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

### This acceptable use policy is intended to ensure:

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

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

### Acceptable Use Policy Agreement

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

### For my professional and personal safety:

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

28

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

* I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
* I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published
* I will only use social networking sites in school in accordance with the school’s policies. I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
* I will not engage in any on-line activity that may compromise my professional responsibilities.

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

* When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
* I will not use personal email addresses on the school ICT systems.
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will ensure that my data is regularly backed up, in accordance with relevant school policies.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
* I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
* I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
* I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

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

Staff/Volunteer Name:

Signed:

Date:

Appendix B

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

Group:

Date:

Reason for investigation:

#### Details of first reviewing person

Name:

Position:

Signature:

#### Details of second reviewing person

Name:

Position:

Signature:

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

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

#### Conclusion and Action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

Appendix C

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Reporting Log Group: | | | | | | |
| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Appendix D

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Training Needs Audit Log Group: | | | | |
| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Appendix E

**STYAL PRIMARY SCHOOL**

Year 1 and Year 2 Pupils

|  |  |
| --- | --- |
| MCj04414710000[1]  Using Computing Equipment in school | * I will use school devices (PCs, laptops, tablets/ ipads) for my learning. * I will ask a teacher before using a device and ask for help if I can’t work the device. * I will only use activities that a teacher has told or allowed me to use. * I will ask a teacher if I am not sure what to do or I think I have done something wrong. * I will look after the school’s computing equipment and tell a teacher if something is broken or not working properly. |
| MCj04414650000[1]  My Online Safety | * I will always use what I have learned about Online Safety to keep myself safe. * I will tell a teacher if I see something that upsets me on the screen. |
| computer_accept  Online Activity in School | * I will only use the internet when the teacher says I can. * I will only go on websites that my teacher allows me to. * I will tell my teacher if I go on a website by mistake. |
| computer_accept  Online Activity at Home | * I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) * Where I have my own username and password, I will keep it safe and secret. * I will tell a trusted adult if I see something that upsets me on the screen.   **My use of Social Media and Gaming**   * I understand that certain sites and games have age restrictions to keep me safe. * I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying. |

Staying Safe Online Agreement

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Child’s Signature**

Parents / Carers:

I know that my son / daughter has signed a Staying Safe Online Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

**I understand that my son’s / daughter’s activity on the ICT systems in school will be monitored and that the school will contact me if they have concerns about any possible breaches of the Staying Safe Online Agreement.**

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.**

**I will monitor my child’s online activity, on whichever device they use, including the apps that they are accessing.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Parent/Carer’s Signature** **Date**

Appendix F

**STYAL PRIMARY SCHOOL**

Year 3 and Year 4 Pupils

Staying Safe Online Agreement

|  |  |
| --- | --- |
| MCj04414710000[1]  Using Computing Equipment in school | * I will use school devices (PCs, laptops, LBQ tablets/ iPads) for my learning. * I will ask a teacher before using a device and ask for help if I can’t work the device. * I will only use activities that a teacher has told or allowed me to use. * I will ask a teacher if I am not sure what to do or I think I have done something wrong. * I will look after the school’s computing equipment and tell a teacher if something is broken or not working properly. * When logging on using my own username and password, I will keep it safe and secret. * I will save only school work on the school computer and will check with my teacher before printing. * I will log off or shut down a computer when I have finished using it. |
| computer_accept  Online Activity in School | * I will only visit sites that my teacher has told me that I should use   **My School Accounts**   * I will keep my username and password safe and secure - I will not share it. * I will not try to use any other person’s username and password. * I understand that I should not write down or store a password where it is possible that someone may use it.   **My role as a Digital Citizen.**   * I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. * I will respect other people’s work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission. |
| computer_accept  Online Activity at Home | * I will not give out or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) * I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line straight away, to a trusted adult or websites that help keep children safe eg: CEOP, Childnet, Childline, Barnardos   **My Communications**   * I will be aware of the rules we have learnt about in school when I am communicating online. * I will be polite and responsible when I communicate with others. * I will not use inappropriate language and I understand that others may have different opinions.   **My use of Social Media and Gaming**   * I understand that certain sites and games have age restrictions to keep me safe. * I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying. |

I understand that the school also has the right to give me a consequence in school if I am involved in incidents of inappropriate behaviour, that are covered in this agreement. I understand that this applies even if these incidents take place when I am out of school where they involve the school or anyone linked to the school (examples could include cyber-bullying, use of images without permission or sharing personal information).

I understand that these rules, help me to stay safe and I agree to follow them.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Child’s Signature**

Parents / Carers:

I know that my son / daughter has signed a Staying Safe Online Agreement and has received, or will  receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

**I understand that my son’s / daughter’s activity on the ICT systems in school will be monitored and that the school will contact me if they have concerns about any possible breaches of the Staying Safe Online Agreement.**

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.**

**I will monitor my child’s online activity, on whichever device they use, including the apps that they are accessing.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Parent/Carer’s Signature** **Date**

Appendix G

**STYAL PRIMARY SCHOOL**

Year 5 and Year 6 Pupils

Staying Safe Online Agreement

|  |  |
| --- | --- |
| MCj04414710000[1]  Using Computing Equipment in school | * I will use school devices (PCs, laptops, LBQ tablets/ iPads) for my learning. * I will ask a teacher before using a device and ask for help if I can’t work the device. * I will only use activities that a teacher has told or allowed me to use. * I will ask a teacher if I am not sure what to do or I think I have done something wrong. * I will look after the school’s computing equipment and tell a teacher if something is broken or not working properly. * When logging on using my own username and password, I will keep it safe and secret. * I will save only school work on the school computer and will check with my teacher before printing. * I will log off or shut down a computer when I have finished using it. |
| computer_accept  Online Activity in School | * I will only visit sites that are appropriate to my learning at the time * I will not use my mobile phone whilst on the school grounds (if I bring one into school)   **My School Accounts**   * I will keep my username and password safe and secure - I will not share it. * I will not try to use any other person’s username and password. * I understand that I should not write down or store a password where it is possible that someone may steal it.   **My role as a Digital Citizen.**   * I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. * I will respect other people’s work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission. * I will not take or distribute images of anyone without their permission. |
| computer_accept  Online Activity at Home | * I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) * If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. * I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos.   **My Communications (Including texting and messaging)**   * I will be aware of “stranger danger”, when I am online. * I will be polite and responsible when I communicate with others. * I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.   **My use of Social Media and Gaming**   * I understand that certain sites and games have age restrictions to keep me safe. * I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying. |

I understand that the school also has the right to give me a consequence in school if I am involved in incidents of inappropriate behaviour, that are covered in this agreement. I understand that this applies even if these incidents take place when I am out of school where they involve the school or anyone linked to the school (examples could include cyber-bullying, use of images without permission or sharing personal information).

I understand that these rules, help me to stay safe and I agree to follow them.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Child’s Signature**

Parents / Carers:

I know that my son / daughter has signed a Staying Safe Online Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

**I understand that my son’s / daughter’s activity on the ICT systems in school will be monitored and that the school will contact me if they have concerns about any possible breaches of the Staying Safe Online Agreement.**

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.**

**I will monitor my child’s online activity, on whichever device they use, including the apps that they are accessing.**

**I understand that all social media platforms, including TikTok, Snapchat, Instagram, YouTube and others, have a minimum user age limit to create an account (generally between 13 and 16). I am aware that children are breaking the agreements for these sites, and potentially putting themselves at risk by using these sites whilst underage.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Parent/Carer’s Signature** **Date**

1. Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school. [↑](#footnote-ref-1)
2. **The school should add below any specific requirements about the use of mobile/personal devices in school** [↑](#footnote-ref-2)