St. Andrew’s Primary School



Online Safety Policy

## Contents

Development, Monitoring and Review of Policy…………………………………………………..3

Roles and Responsibilities…………………………………………………………………………..5

Policy Statements……………………………………………………………………………………9

Use of Digital Images and Videos…………………………………………………………………11

Data Protection………………………………………………………………………………………12

Communications…………………………………………………………………………………….14

Social Media – Protecting Professional Identity………………………………………………….15

Incidents……………………………………………………………………………………………...16

School Actions and Sanctions……………………………………………………………………..17

## Development, Monitoring and Review of this Policy

4

This online safety policy has been developed by a working group made up of:

* Headteacher and Senior Leaders
* Online Safety Lead
* Staff – including teachers and support staff
* Governors
* Parents and carers
* Pupils

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

### Schedule for Development/Monitoring/Review

5

|  |  |
| --- | --- |
| This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on: |  |
| The implementation of this online safety policy will be monitored by: | *Senior Leadership Team* |
| Monitoring will take place at regular intervals: | *Informally termly, policy will be updated annually or when new legislation is brought in.* |
| The Board of Directors/Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Informally through termly meetings where necessary and formally annually.* |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | *September 2022* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *St. Andrew’s Safeguarding Officers: Mrs J. Giles, Mrs E. Charles, Mrs K. Small and Mrs R. Harrod.*  *Online Safety Lead: Miss E. Davies*  *Designated Governors*  *The Local Authority*  *The Police where necessary* |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Monitoring data and logs of internet activity (including sites visited)/filtering reports provided by SRS
* Surveys/questionnaires of
  + Learners
  + Parents/carers
  + Staff

### Scope of the Policy

This policy applies to all members of the St. Andrew’s community (including staff, learners, volunteers, parents/carers, visitors and community users) who have access to and are users of our digital technology systems, both in and out of St. Andrew’s.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of learners when they are off the St. Andrew’s 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 St. Andrew’s, but is linked to membership of the school community.

St. Andrew’s 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

The following section outlines the online safety roles and responsibilities of individuals and groups within St Andrew’s Primary School:

### 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 Governors receiving regular information about online safety incidents and monitoring reports where necessary. A member of the ***Governing Body (name)*** has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

* Meetings with the Online Safety Lead (Miss E. Davies)
* Attendance at an Online Safety Group meeting
* Monitoring of online safety incident logs or filtering logs alongside Online Safety Coordinator where necessary

6

### 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.
* The Headteacher and at least another member of the Senior Leadership Team 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.
* The Headteacherand Senior Leadersare responsible for ensuring that theOnline Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* The Headteacher 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.
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

### Online Safety Lead

* Leads the Online Safety Group.
* Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.
* Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* Provides training and advice for staff.
* Liaises with the Local Authority and relevant bodies.
* Liaises with 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 logs.
* Attends relevant meetings of Governing Body.
* Reports regularly to Senior Leadership Team.

### Network Manager and Technical Staff

The Network Manager and Technical Staff (SRS) are responsible for ensuring that:

* St. Andrew’s technical infrastructure is secure and is not open to misuse or malicious attack.
* St. Andrew’s meets required online safety technical requirements and any online safety policies or guidance provided by the Local Authority or other relevant body.
* 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.
* 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.
* The use of the networks, internet and digital technologies is regularly monitored in order that any misuse or attempted misuse can be reported to theHeadteacher *and* Online Safety Leadfor investigation.
* Monitoring software and 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 online safety policy and practices.
* They have read, understood and signed the staff acceptable use policy.
* They report any suspected misuse or problem to the Headteacher/Relevant Senior Leader/Online Safety Lead for investigation.
* All digital communications with learners and 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.
* Learners understand and follow the online safety policy and acceptable use policies.
* Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* They monitor the use of digital technologies and toolkits and implement current policies with regard to these devices.
* During sessions where internet use is pre-planned, learners 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/Designated Person/Officer

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 online 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 St. Andrew’s community, with responsibility for issues regarding online safety and the monitoring of the policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Lead with:

* The production, review and monitoring of the online safety policy.
* Consulting stakeholders – including parents/carers and the learners about the online safety provision.
* Monitoring improvement actions identified through use of the 360 degree safe self-review tool.

### Learners

* are responsible for using digital technology systems in accordance with our acceptable use agreement.
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
* will be expected to know and understand policies on the use of digital devices. 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 St. Andrew’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 digital devices in an appropriate way. St. Andrew’s will take every opportunity to help parents understand these issues through parent consultations, newsletters, website posts, social media posts, information about national and local online safety campaigns and literature as well as online safety sessions*.*  Parents and carers will be encouraged to support St. Andrew’s in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken.
* any social media presence.
* correspondence with others online.

### Community Users

Community Users who access St. Andrew’s systems or programmes as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to St. Andrew’s systems.

## Policy Statements

### Education – Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety/digital literacy is therefore an essential part of St. Andrew’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.

To ensure this:

* A planned online safety curriculum should be provided as part of our St. Andrew’s curriculum and should be regularly revisited.
* Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
* Learners should be taught in all sessions to be critically aware of the content they access online and be guided to validate the accuracy of information.
* Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
* Learners 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. This is due to the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
* Learners should be helped to understand the need for the 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 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 or regulation of 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.

St. Andrew’s will therefore seek to provide information and awareness to parents and carers through:

* Curriculum activities
* Letters, newsletters, information through our website
* Parents/carers consultations
* High profile events/campaigns e.g. Safer Internet Day
* Reference to relevant web sites/publications

### Education – The Wider Community

St. Andrew’s will provide opportunities for our wider school community to gain from our online safety knowledge and experience. This may be offered through the following:

* Providing family learning courses in use of new digital technologies, digital literacy and online safety
* Online safety messages targeted towards grandparents and other relatives as well as parents.
* Our website will provide online safety information for the wider community
* Collaborating within our Cluster and beyond

### 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.
* All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the St. Andrew’s online safety policy and acceptable use agreements.
* It is expected that some staff may 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 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 staff meetings and/or training sessions.
* The Online Safety Lead will provide advice, guidance and training to individuals as required.

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

St. Andrew’s is responsible for ensuring that the school infrastructure and 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:

* Technical systems will be managed in ways that ensure that St. Andrew’s meets recommended technical requirements
* There will be regular reviews and audits of the safety and security of St.Andrews’ technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to St. Andrew’s technical systems and devices
* All users will be provided with a username and secure password by SRS who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
* Digital Lead is responsible for liaising with SRS to ensure that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
* Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
* Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. This is due to the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
* St. Andrew’s regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
* 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 regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
* An agreed policy is in place that 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/CDs/DVDs) 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.

### Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners 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 learners 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 learners 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 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 on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
* Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow St. Andrew’s 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 learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Learners must not take, use, share, publish or distribute images of others without their permission.
* Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
* Learners’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Learners’ work can only be published with the permission of the learner and parents/carers.

### Data Protection

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

#### St. Andrew’s 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.
* 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).
* 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/academy 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 72 hours 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.
* 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.

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 sensitive 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. When using communication technologies, St. Andrew’s considers the following as good practice:

* Users must immediately report 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 learners or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
* Learners 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 St. Andrew’s website and only official email addresses should be used to identify members of staff.

### 

### Social Media – Protecting Professional Identity

St. Andrew’s 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.

St. Andrew’s staff ensure that:

* No reference should be made in social media to learners, parents/carers or St. Andrew’s 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.

#### For official school social media accounts there is:

* 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.
* Systems for reporting and dealing with abuse and misuse.
* Understanding of how incidents may be dealt with under St. Andrew’s disciplinary procedures.

#### 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 which St. Andrew’s endeavours to do regularly.
* The school should effectively respond to social media comments made by others according to a defined policy or process.

St. Andrew’s use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

## Incidents

It is hoped that all members of the St. Andrew’s 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.
* 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 or relevant organisation.
  + 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. It will 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 and Sanctions

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Actions/Sanctions** | | | | | | | | |  |
| Learner Incidents | Refer to class teacher | Refer to Progression Step Lead | Refer to Headteacher/Deputy Headteacher | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Warning/RTO | Further sanction e.g. internal exclusion | Refer to Safeguarding Team | Refer to Police |
| **Deliberately accessing or trying to access material that could be considered illegal** |  | X | X | X | X |  | X |  |  |  |
| Unauthorised use of non-educational sites during lessons (First offence) | X | X |  |  |  |  |  |  |  |  |
| Unauthorised/inappropriate use of iPad/digital camera/other mobile device | X | X |  |  | X |  | X |  |  |  |
| Unauthorised/inappropriate use of social media/ messaging apps/personal email |  | X | X |  | X |  |  |  |  |  |
| Attempting to access or accessing the St. Andrew’s network, using the account of a member of staff | X | X | X |  | X |  | X |  |  |  |
| Corrupting or destroying the data of other users | X |  |  |  |  |  |  |  |  |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | 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 |  |  |
| 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 |  |

|  | | **Actions/Sanctions** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Staff Incidents | Refer to line manager/PS Lead | | Refer to Headteacher/Deputy | Refer to Local Authority/HR | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action | Refer to Police |
| **Deliberately accessing or trying to access material that could be considered illegal.** |  | | X | X | X | X |  | X |  |
| Inappropriate personal use of the internet/social media/personal email | 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 |  |  |  |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | | X | X |  | X |  | X |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | | X | X |  | X |  | X |  |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils | X | | X | X |  |  |  |  |  |
| 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 |  | X |  |
| Using proxy sites or other means to subvert the school’s filtering system |  | | X |  | X |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  | | X | X | X | X |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  | | X | X | X |  |  | X | X |
| Breaching copyright or licensing regulations |  | | X |  | X | X |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions |  | | X | X |  |  |  | X |  |