***A house with a roof

Description automatically generated*St** Andrew’s School

A school with Quaker values

Aylmerton Hall ⬩ Holt Road

Aylmerton ⬩ Norfolk ⬩ NR11 8QA

Telephone: 01263 837927

Email: [head@standrewsschool.co.uk](mailto:head@standrewsschool.co.uk)

.

**The St Andrew’s School Trust is a Registered Charity No. 1129232**

Online Safety

Policy

Last reviewed date: Summer Term 2024

Adopted by Trustees date: 15th July 2024

Next review date: Summer Term 2025

## Development, Monitoring and Review of this Policy

4

This Online Safety policy has been developed by a working group made up of:

* Head
* Senior Management Team
* Staff
* Trustees

Consultation has taken place through a range of formal and informal meetings.

## Schedule

5

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | This Online Safety policy was approved by the Trustees on: |  | | | The implementation of this Online Safety policy will be monitored by the: | Online Safety Lead, DSLs, Senior Management Team, Trustee responsible for Safeguarding, IT Teacher. | | Monitoring will take place at regular intervals: | Termly | | The Trustees 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: | During Trustees Meetings, alongside the Safeguarding Reports. | | 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: | Summer 2025 | | Should serious online safety incidents take place, the following external persons / agencies should be informed: | LA Safeguarding Officer, LADO, Police, Wavenet. | |  |  |
|  |  |  |

The school will monitor the impact of the policy using:

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

6

## Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) 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 Head to such extent as is reasonable, to regulate the behaviour of students when they are off the schoolsite 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 regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents 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 the school:

## 3.1 Trustees

The Trusteesare responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about online safety incidents and monitoring reports. A member of the Trusteeshas taken on the role of Online Safety Governor, alongside the role of Safeguarding Trustee. The role of the Online Safety Trustee will include:

* regular meetings with the Online Safety Lead and DSLs
* regular monitoring of online safety incident logs
* reporting to relevant Trustees

## 3.2 Head and Senior Management Team

* The Head have a duty of care for ensuring the safety (including online safety) of members of the school community. The day-to-day responsibility for online safety will be delegated to the Online Safety Lead who currently is the Safeguarding and Welfare Manager.
* The Head and all members of the Senior Management 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 (see flow chart on dealing with online safety incidents included in a later section, “Responding to incidents of misuse”, and relevant Local Authoritydisciplinary procedures).
* The Head / Online Safety Lead and Senior Management Team are responsible for ensuring that other relevant staff receive suitable training to enable them to carry out their online safety roles as relevant.
* The Head / Online Safety Lead and Senior Management Team 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 support to those colleagues who take on important monitoring roles.
* The Senior Management Team (DSLs) will receive regular monitoring reports from the Head / Online Safety Lead.

## 3.3 Online Safety Lead

* leads the Online Safety for the school community
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* provides training and advice for staff
* liaises with the Local Authority and Wavenet Technologies
* liaises with school technical staff
* receives reports of any online safety incidents and creates a log of incidents to inform future online safety developments
* meets regularly with Online Safety Trustee and DSLs to discuss current issues, review incident logs and filtering / change control logs
* attends relevant meetings of Trustees
* reports regularly to Senior Management Team

## 3.4 Network Manager / Technical staff

It is the responsibility of the school, primarily the Head Teachers and Online Safety Lead, to ensure that the managed service provider (Wavenet) carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy and procedures.

The Network Manager, Technical Staff and Co-ordinator for ICT are responsible for ensuring:

* that the school meets online safety technical requirements and any Local Authority or other relevant Online Safety Policy that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
* the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
* that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
* that the use of the network / Internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head / Online Safety Lead or Senior Management Team for investigation / action / sanction
* that monitoring software / systems are implemented and updated as agreed in school policies

## 3.5 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 Head / Online Safety Lead or Senior Management Team for investigation/action/sanction
* all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
* Staff should act as good role models in their use of digital technologies, the Internet and mobile devices.
* online safety issues are embedded in all aspects of the curriculum and other activities
* students understand and follow the Online Safety Policy and acceptable use policies
* students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices
* in lessons where Internet use is pre-planned students 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

## 3.6 Designated Safeguarding Leads

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
* exposure to extremist ideology and/or radicalisation materials

## 3.7 Students

* are responsible for using the school digital technology systems in accordance with the Student 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 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

## 3.8 Parents / Carers

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

* digital and video images taken at school events
* access to any parents’ online groups
* their children’s personal devices in the school (where this is allowed)

# Policy Statements

## 4.1 Education – Students

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

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

* A planned online safety curriculum should be provided as part of Computing/Life Skills Lessons and other lessons and should be regularly revisited
* Key online safety messages should be reinforced as part of a planned programme of Life Skills Lessons, morning quiet time and ICT lessons
* Students should be taught in all lessons to be critically aware of the materials/content they access online and to be guided to validate the accuracy of the information
* Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
* Students 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 should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
* In lessons where Internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable fortheir use.
* Where students are allowed to 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.

## 4.2 Education – Parents / Carers

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

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

* Curriculum activities
* Letters, newsletters, web site
* Parents/Carers sessions
* 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>

## 4.3 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 school Online Safety Policy and Acceptable Use Agreements.
* It is expected that some staff will identify online safety as a training need within their individual appraisal process.
* The Online Safety Lead will receive regular updates through attendance at external training events (e.g., from LA and other relevant organisations) 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 /training days.
* The Online Safety Lead will provide advice/guidance/training to individuals as required.

4.4 Training - Trustees

Trustees should have an awareness of online safety. This may be offered in a number of ways:

* Attendance at training provided by the Local Authority or any other relevant organisation.
* Participation in school training and information sessions for staff or parents.

4.5 Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school, primarily the Head and Online Safety Lead, to ensure that the managed service provider (Wavenet) carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. It is also important that the managed service provider is fully aware of the school Online Safety Policy and Procedures and the Acceptable Use Policy. The school should also check their Local Authority policies on these technical issues.

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 the school technical systems by Wavenet
* 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 by Wavenet who will keep an up-to-date record of users and their usernames.Users are responsible for the security of their username and password and will be required to change their password every year*.*
* The “master / administrator” passwords for the school ICT systems, used by the Network Manager must also be available to the Head or other nominated senior leader on demand.
* Wavenet are 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. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
* 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. The process to deal with requests for filtering changes is to contact the office first. If it is authorised, the office will then contact Wavenet to implement the change. This will be logged.
* Internet filtering / monitoring should ensure that students are safe from terrorist and extremist material when accessing the Internet.
* The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for different ages / stages and different groups of users – staff / students etc.
* An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. They need to contact the office directly by telephone and report the incident/breach to Carol McKean (Online Safety Lead) or Julie Jackson (Data Protection Lead).
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are monitored by Wavenet. The school infrastructure and individual workstations are protected by up-to-date virus software.
* There is agreed provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the school systems with security levels appropriate to that role.
* An agreement letter is in place detailing the extent of personal use and responsibility of, that users (staff / students) and their family members are allowed on school devices that may be used out of school e.g., laptops.
* Staff are not permitted to download executable files or install programmes on school devices without express permission from Wavenet and/or the Office.
* An agreed policy is in place (Data Protection Policy) regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on school devices.

4.6 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include smartphones, tablets, 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 of mobile / personal devices in a school context is educational. The mobile devices policy should be consistent with and interrelated to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy.

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, students and parents / carers will consider the use of mobile technologies

The school allows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | School Devices | | | Personal Devices | | |
|  | **School owned for single user** | **School owned for multiple users** | **Authorised device** | **Student owned** | **Staff**  **owned** | **Visitor owned** |
| Allowed in school | *Yes* | *Yes* | *Yes* | *No* | *Yes* | *Yes* |
| Full network access | *Yes* | *Yes* | *Yes* | *No* | *No* | *No* |
| Internet only | *Yes* | *Yes* | *Yes* | *No* | *Yes*  *(via BYOD separate network)* | *Yes*  *(via BYOD separate network)* |

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

4.7 School owned / provided devices:

* Classes/students have been allocated devices and a record is kept in the office. Mobile phones are available to take out with the mini-buses and the teacher in charge will be responsible for it.
* Mobile devices that belong to school are only to be used for school purposes, both in and out of school.

Personal use of school mobile devices is not authorised unless in an emergency.

* Access to the school network is authorised for remote access for office staff and senior management. Internet access is authorised for any school use and for students whilst being monitored. There is a separate network for BYODs.
* Management of devices, installation of apps, changing of settings and monitoring are managed by Wavenet and the office staff.
* Network / broadband capacity is monitored via the office and streaming is timetabled to prevent overload of the system as much as viable.
* Wavenet provide technical support, and any issues are directed to them via the office. For in-house support, the IT teacher and office are available.
* Wavenet set the filtering systems on devices used by the school via the Network. Staff are encouraged to install their own filtering systems on their personal devices.
* Staff use One Drive, and the accounting and payroll software is cloud based.
* St Andrews has a Data Protection Policy and any breaches of this are reported to Julie Jackson in the office.
* Images relating to the school are stored securely on the Network and the teachers are responsible for their subject related images. Parents are asked to give or deny consent for their children’s images to be shared on school related newsletters/papers. A central record is kept of who is allowed to have their photograph taken.
* Exit processes – The office and Wavenet work together to block network access of staff or students who have left, clean devices of old files, migrate data over and then decide on what happens to the remaining data.
* Deliberate damage of school owned devices lies with the user, and they are financially liable for repairs or replacement. Accidental damage is covered by school. Personal devices belonging to students, parents or staff are the owner’s responsibility and damage /replacement costs will not be met by the school.
* Staff receive regular training in online safety.

4.8 Personal devices:

* Staff / students / visitors may bring their personal devices to school. Staff can use their devices whilst in school during their own break time, not however, whilst in the vicinity of students. Professional visitors may be permitted to use their devices in school during meetings or similar if relevant to the situation. Other visitors will be asked to refrain from using their devices whilst on site. They are not permitted to take photographs or videos or any recordings (see Mobile Device Policy).
* Students can bring in their devices on the understanding they hand them over for safekeeping on arrival at school. They will be returned at the end of the school day and should not be switched back on until they are in their vehicle for returning home. The devices will be locked away within the student’s classroom in a safe cabinet.
* Staff are permitted to use mobile devices for school business following the Mobile Device Policy.
* Staff using their own devices will be on a separate network and can obtain the password from the office to enable access. This password should not be shared amongst staff.
* The network / broadband capacity will be monitored from the office and staff are asked to refrain from over-usage which could impact on lessons/remote learning.
* Technical support for personal devices can be requested via the office. It may be refused depending on the requirements of the user and the time factor involved.
* Data Protection – all staff will undertake Data Protection training and are expected to maintain high levels of security. If a breach occurs, staff are required to alert the office immediately. Julie Jackson will advise on how to report the Data Breach and will log it for our records.
* Senior staff have the right to take, examine and search users’ devices in the case of misuse (see Behaviour Policy).
* Staff/visitors/students are not permitted to take any photographs, videos or recordings whilst in school on their personal devices.
* Personal devices must be clearly labelled in order to be easily identified. School is not responsible for any loss, theft or damage to personal devices. Personal devices are the sole responsibility of the owner.
* Visitors will be informed about school requirements via the school website, posters in the foyer by the visitors signing in sheets and when greeted by the office staff or staff members. This will also be covered during the ‘New Parents and Students Induction’ when the student starts at St Andrew’s School.
* The School Online Safety education programme teaches the students about safe use of mobile devices and what steps to take to report any misuse. This is repeated throughout the curriculum over the academic year. The local community police team also deliver safer use of mobile devices and technology presentations.

## Use of digital and video images

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

* When using digital images, staff should inform and educate students 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 are published on the school website / social media / local press
* Staff and volunteers are allowed to take digital / video images to support educational aims, e.g., as part of lesson content, 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 are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Students must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
* Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Students’ work can only be published with the permission of the student 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 and a Data Protection Officer, currently Julie Jackson.
* It has paid the appropriate fee to the Information Commissioner’s Office (ICO).
* It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
* Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
* The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice (School welcome pack).
* Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
* It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g., cloud service providers.
* Procedures must be in place to deal with the individual rights of the data subject i.e., a Subject Access Request to see all or a part of their personal data held by the data controller.
* There are clear and understood data retention policies and routines for the deletion and disposal of data.
* There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
* Consideration has been given to the protection of personal data when accessed using any remote access solutions.
* All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
* All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimisingthe risk of its loss or misuse.

* Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
* Transfer data using encryption and secure password protected devices.

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

* The data must be encrypted, and password protected.
* The device must be password protected. Many memory sticks / cards and other mobile devices cannot be password protected.
* The device must offer approved virus and malware checking software.

16

* The data must be securely deleted from the device once it has been transferred or its use is complete.

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The table below details allowances

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Staff** | | **Students** | |
|  | Allowed | Not Allowed | Allowed | Not Allowed |
| Mobile phones may be brought to the school |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |
| Use of mobile phones in personal break time |  |  |  |  |
| Use of school email address for personal emails |  |  |  |  |
| Use of social media whilst on site or during school hours |  |  |  |  |

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

* The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
* Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Any digital communication between staff, students and parents / carers (email, social media, chat, blogs, 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 will be provided with individual school email addresses for educational use.
* Students 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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, 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 students, 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, parents / carers or school staff
* They do not engage in online discussion on personal matters relating to members of the school community
* Personal opinions should not be attributed to the school or local authority
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use:

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

8.1 Monitoring of Public Social Media

* As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
* The school will effectively respond to social media comments made by others by following the relevant process

## 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. Staff should use their professional judgement and online safety training knowledge to ensure their conduct, as well as the conduct of other users, upholds the values and ethos of the school. If staff have reason to believe that this has been compromised in any way, they should follow the school’s reporting procedures.

## 9.1 Illegal Incidents

If there is any suspicion that the website(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.

**Illegal Incidents Flowchart**



## 9.2 Other Incidents of Misuse

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 SMT 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 national / local organisation (as relevant).
  + Police involvement and/or action
* If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  + incidents of ‘grooming’ behaviour
  + the sending of obscene materials to a child
  + adult material which potentially breaches the Obscene Publications Act
  + criminally racist material
  + promotion of terrorism or extremism
  + other criminal conduct, activity or materials
* Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

## 9.3 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.

|  |
| --- |
|  |

Appendices

22

Appendix 1

# Student Acceptable Use Agreement Template – for older students

### School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe Internet access at all times.

#### This Acceptable Use Agreement is intended to ensure:

* that young people will be responsible users and stay safe while using the Internet and other digital 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 will have good access to digital technologies to enhance their learning and will, in return, expect the students 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.

#### For my own personal safety:

* I understand that the schoolwill monitor my use of the systems, devices and digital communications.
* I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will be aware of “stranger danger” when I am communicating on-line.
* I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
* 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.

#### I understand that everyone has equal rights to use technology as a resource and:

* I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
* 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 use the schoolsystems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g., YouTube), unless I have permission of a member of staff to do so.
* I will act as I expect others to act toward me.
* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

#### I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

* I will only use my own personal devices (mobile phones / USB devices etc) during the journey to and from school. I understand that, if I do use my own devices on the journey, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
* I will not use social media sites whilst at school.

#### When using the Internet for research or recreation, I recognise that:

* I should ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not try to download copies (including music and videos)
* When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

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

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

# Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, which is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

* I use the schoolsystems and devices (both in and out of school)
* I only use my own devices on the journey to and from school and not whilst in school e.g., mobile phones, gaming devices USB devices, cameras etc.
* I use my own equipment out of the school in a way that is related to me being a member of this schoole.g., communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student:

Class:

Signed:

Date:

Name of Parent/Carer

Signed:

Date:

# Appendix 2

# Student Acceptable Use Policy Agreement Template – for younger pupils

#### This is how we stay safe when we use computers:

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

Signed (student):

Date: ……………………………………………………..

Signed (parent/carer):

Date: …………………………………………………….

# 

# Appendix 3

# 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’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 schoolwill 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, VLE 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 ICT 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. Where these images are published (e.g., on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
* I will not use social networking sites in school in accordance with the school’s policies.
* I will only communicate with students 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 (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using schoolequipment. I will also follow any additional rules set by the schoolabout 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 not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
* I will 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 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 / 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 Protected and Restricted data must be held in lockable storage.
* I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

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

Staff / Volunteer Name:

Signed:

Date:

# Appendix 4

# Responding to incidents of misuse – flow chart



# 

# Appendix 5

# 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

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Reporting Log – St. Andrew’s School Group: | | | | | | | | Date | Time | Incident | Action Taken | | Incident Reported By | Signature | | What? | By Whom? | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  Appendix 6 |