**Alderley Edge Community Primary School**

# Online Safety Policy

This policy applies to all members of the schoolcommunity (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Version: 1

Replaced previous Acceptable Use Policy

Date created: [24/1/23]

Next review date: [24/3/25]

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Alderley Edge Community Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached ‘Legislation’ Appendix.

**This Online Safety Policy applies to all members of the schoolcommunity (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).**

Alderley Edge Community Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

## Schedule for development, monitoring and review

5

|  |  |
| --- | --- |
| This Online Safety Policy was approved by the *school* *governing body on:* | March 2023 |
| The implementation of this Online Safety Policy will be monitored by: | Head Teacher |
| Monitoring will take place at regular intervals: | Annually |
| The *governing body* 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: | Annually  |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | 24.3.24 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | Cheshire East Local Authority Cheshire East LADOCheshire Police |

## Process for monitoring the impact of the Online Safety Policy

5

The school will monitor the impact of the policy using:

* *logs of reported incidents*
* *monitoring logs of internet activity (including sites visited)*
* *internal monitoring data for network activity*

# Policy and leadership

## Responsibilities

6

7

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[[1]](#footnote-1)and groups within the school.

### Headteacher and senior leaders

* The headteacherhas a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety.
* 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[[2]](#footnote-2).
* The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
* The headteacher/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.

### Governors

The DfE guidance “Keeping Children Safe in Education” states:

“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare …. this includes … online safety”

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy [e.g. by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”](https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board).

This review will be carried out by the Assets Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of GDPR and Online Safety Governor to include:

* termly meetings with the Head Teacher
* regularly receiving (collated and anonymised) reports of online safety incidents
* checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
* reporting to relevant governors committee

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

### Online Safety Lead

At Alderley Edge Community Primary School, the Online Safety Lead is the Head Teacher

The Online Safety Lead will:

* take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
* have a leading role in establishing and reviewing the school online safety policies/documents
* promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
* liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
* ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
* receive reports of online safety incidents and create a log of incidents to inform future online safety developments
* provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
* liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
* meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
* attend relevant governing body meetings/groups
* report regularly to headteacher/senior leadership team.
* liaises with the local authority/MAT/relevant body.

### Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education” states:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder’s job description.” … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college.”

TheDesignated Safeguarding Lead will be trained in online safety issues and be aware of the potential for serious 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.

### Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme e.g. [ProjectEVOLVE](http://www.projectevolve.co.uk/) and Purple Mash.

This will be provided through:

* a discrete programme
* PHSE and SRE programmes
* A mapped cross-curricular programme
* assemblies and pastoral programmes
* through relevant national initiatives and opportunities e.g. [Safer Internet Day](https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2022) and [Anti-bullying week](https://www.anti-bullyingalliance.org.uk/anti-bullying-week).

### Teaching and support staff

School staff are responsible for ensuring that:

* they have an awareness of current online safety matters/trends and of the current schoolOnline Safety Policy and practices
* they understand that online safety is a core part of safeguarding
* they have read, understood, and signed the staff acceptable use agreement (AUA)
* they immediately report any suspected misuse or problem to the Head Teacher for investigation/action, in line with the school safeguarding procedures
* 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 and other activities
* ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they supervise and 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 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*
* where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [SWGfL Safe Remote Learning Resource](https://swgfl.org.uk/resources/safe-remote-learning/)
* have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
* they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

### Network manager/technical staff

Thenetwork manager (currently supplied by Virtue Technologies) is responsible for ensuring that:

* they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
* the school technical infrastructure is secure and is not open to misuse or malicious attack
* the schoolmeets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
* there is clear, safe, and managed control of user access to networks and devices
* 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 technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Head Teacherfor investigation and action
* the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
* monitoring software/systems are implemented and regularly updated as agreed in school policies

### Learners

* are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (a children’s version is available on the school website and in classrooms)
* should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* should know what to do if they or someone they know feels vulnerable when using online technology
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’sOnline Safety Policy covers their actions out of school, if related to their membership of the school.

### Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

* publishing the school Online Safety Policy on the school website
* providing them with a copy of the learners’ acceptable use agreement
* publish information about appropriate use of social media relating to posts concerning the school
* seeking their permissions concerning digital images, cloud services etc
* parents’/carers’ evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

* reinforcing the online safety messages provided to learners in school

### Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. (A community user’s acceptable use agreement template can be found in the appendices).

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

# Policy

11

## Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

**“Online safety** and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

* sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
* allocates responsibilities for the delivery of the policy
* is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
* establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
* describes how the school will help prepare learners to be safe and responsible users of online technologies
* establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
* is supplemented by a series of related acceptable use agreements
* is made available to staff at induction and through normal communication channels
* is published on the school website.

## Acceptable use

### The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

|  User actions18 | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| --- | --- | --- | --- | --- | --- |
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:*** Child sexual abuse imagery\*
* Child sexual abuse/exploitation/grooming
* Terrorism
* Encouraging or assisting suicide
* Offences relating to sexual images i.e., revenge and extreme pornography
* Incitement to and threats of violence
* Hate crime
* Public order offences - harassment and stalking
* Drug-related offences
* Weapons / firearms offences
* Fraud and financial crime including money laundering

N.B. Schools should refer to guidance about dealing with self-generated images/sexting – [UKSIC Responding to and managing sexting incidents](https://swgfl.org.uk/assets/documents/managing-sexting-incidents.pdf?_=1554476329) and [UKCIS – Sexting in schools and colleges](https://www.gov.uk/government/publications/sexting-in-schools-and-colleges) |  |  |  |  | **X** |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | * Using another individual’s username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)
* Gaining unauthorised access to school networks, data and files, through the use of computers/devices
* Creating or propagating computer viruses or other harmful files
* Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)
* Disable/Impair/Disrupt network functionality through the use of computers/devices
* Using penetration testing equipment (without relevant permission)

N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information [here](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices) |  |  |  |  | **X** |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school’s filtering practices and/or AUAs) |  |  |  | X |  |
| Promotion of any kind of discrimination |  |  |  | X |  |
| Using school systems to run a private business |  |  |  | X |  |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school  |  |  |  | X |  |
| Infringing copyright |  |  |  | X |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) |  |  | X |  |  |
| Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | X |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |   | **STAFF** |   |   |   | **CHILDREN** |   |   |
|  | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awareness |
| Online gaming |   |   | X |   |   |   |   | X |
| Online shopping/commerce |   |   |   | X | X |   |   |   |
| File sharing |   | X |   |   |   |  |   |  x |
| Social media  |   |   | X |   | X |   |   |   |
| Messaging/chat |   | X |   |   |   |   |   | X |
| Entertainment streaming e.g. Netflix, Disney+ |   |   | X |   | X |   |   |   |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok |   |   | X |   |   |   |   | X |
| Mobile phones may be brought to school |   | X |   |   |   |   |   | X |
| Use of mobile phones for learning at school |   | X |   |   |   |   |   | X |
| Use of mobile phones in social time at school |   | X |   |   | X |   |   |   |
| Taking photos on mobile phones/cameras | X |   |   |   | X |   |   |   |
| Use of other personal devices, e.g. tablets, gaming devices  | X |   |   |   |   |   |   | X |
| Use of personal e-mail in school, or on school network/wi-fi | X |   |   |   | X |   |   |   |
| Use of school e-mail for personal e-mails | X |   |   |   | X |   |   |   |
|  |  |  |  |  |  |  |  |  |

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

* when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
* any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
* staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
* users should immediately report to a 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
* relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

## Reporting and responding

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

*“School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*

* *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse”*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

* **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
* **all members of the school community will be made aware of the need to report online safety issues/incidents**
* **reports will be dealt with as soon as is practically possible once they are received**
* **the Designated Safeguarding Lead will have appropriate skills and training to deal with online safety risks.**
* **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm** (see flowchart and user actions chart in the appendix), **the incident must be escalated through the agreed school safeguarding procedures.**
* any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
* where there is no suspected illegal activity, devices may be checked using the following procedures:
	+ one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
	+ conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
	+ ensure that the relevant staff 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 / MAT (as relevant)
		- police involvement and/or action
* it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
* there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
* incidents should be logged by the Head Teacher
* relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline); [Reporting Harmful Content](https://reportharmfulcontent.com/?lang=en); [CEOP.](http://www.ceop.police.uk/)
* those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
* learning from the incident (or pattern of incidents) will be provided to:
	+ *the Designated Safeguarding Leads group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
	+ *staff, through regular briefings*
	+ *learners, through assemblies/lessons*
	+ *parents/carers, through newsletters, school social media, website*
* *governors, through regular safeguarding updates*
* *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

## Online Safety Incident Flowchart

Unsuitable materials or activity

Illegal materials or activities found or suspected

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to the Designated Safeguarding Lead (DSL) / Head Teacher

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions1.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

Implement changes

Monitor situation

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

### School actions

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.

## Responding to Learner Actions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to class teacher | Refer to Headteacher | Refer to Police/Social Work | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Further sanction, in line with behaviour policy |
| Deliberately accessing or trying to access material that could be considered illegal (see list [in earlier section](#_User_actions) on User Actions on unsuitable/inappropriate activities). |  | X | X |  |  |  |  |
| Attempting to access or accessing the school network, using another user’s account (staff or learner) or allowing others to access school network by sharing username and passwords |  | X |  | X | X |  | x |
| Corrupting or destroying the data of other users. | X | X |  | X | X |  | X |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | X | X |  X (if criminal act inciting hatred) |  | X | X | X |
| Unauthorised downloading or uploading of files or use of file sharing. | X | X |  |  | X |  | X |
| Using proxy sites or other means to subvert the school’s filtering system. | X | X |  |  | 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 | x |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. |  | x |  | x | x |  | x |
| Unauthorised use of digital devices (including taking images) |  | x |  |  | x | X | x |
| Unauthorised use of online services |  | x |  |  | x | X | x |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. |  | x | x | X(public and press relation and legal) | x | X | x |
| Continued infringements of the above, following previous warnings or sanctions. |  | x |  | x | x | X | x |

## Responding to Staff Actions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to Headteacher/ Principal | Refer to local authority/LADO/HR | Refer to Police | Refer to LA / Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list** [**in earlier section**](#_User_actions) **on unsuitable / inappropriate activities)** | **X** | **X** | **X** |  |  |  |  |
| Deliberate actions to breach data protection or network security rules. | **X** |  |  | **X** | **X** |  |  |
| Deliberately accessing or trying to access offensive or pornographic material | **X** | **X** | **X** | **X** |  | **X** | **X** |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | **X** | **X** |  | **X** | **X** | **X** |  |
| Using proxy sites or other means to subvert the school’s filtering system. | **X** | **X** |  | **X** | **X** | **X** |  |
| Unauthorised downloading or uploading of files or file sharing  | **X** | **X** |  | **X** | **X** | **X** |  |
| Breaching copyright or licensing regulations. | **X** | **X** |  | **X** | **X** | **X** |  |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account. | **X** | **X** |  | **X** | **X** |  |  |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | **X** | **X** | X | **X** | **X** | **X** | **X** |
| Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers | **X** | **X** |  | **X** | **X** | **X** |  |
| Inappropriate personal use of the digital technologies e.g. social media / personal e-mail | **X** | **X** |  | **X** | **X** | **X** |  |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner | x |  |  | x | x |  |  |
| Actions which could compromise the staff member’s professional standing | **X** | **X** |  | **X** | **X** | **X** |  |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | **X** | **X** |  | **X** | **X** | **X** |  |
| Failing to report incidents whether caused by deliberate or accidental actions | **X** | **X** |  | **X** | **X** | **X** |  |
| Continued infringements of the above, following previous warnings or sanctions. | **X** | **X** |  | **X** | **X** | **X** | x |

## Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school’s online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for:

*“a carefully sequenced RSHE curriculum, based on the Department for Education’s (DfE’s) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of ‘nudes’..”*

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](http://www.projectevolve.co.uk/) for all year groups matched against a nationally agreed framework e.g. [Education for a Connected Work Framework by UKCIS/DCMS](https://www.gov.uk/government/publications/education-for-a-connected-world) and regularly taught in a variety of contexts.
* Lessons are matched to need; are age-related and build on prior learning
* Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
* Learner need and progress are addressed through [effective planning and assessment](https://projectevolve.co.uk/guidance/knowledge-maps/)
* Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Computing
* it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](https://hwb.gov.wales/zones/keeping-safe-online/safer-internet-day/) and [Anti-bullying week](https://www.anti-bullyingalliance.org.uk/anti-bullying-week)
* the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
* *learners should be helped to understand the need for the learner 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 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*
* *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and 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 should be able to request the temporary removal of 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*
* the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

* *meetings of the School Safety Ambassadors*
* *mechanisms to canvass learner feedback and opinion.*
* *learners designing/updating acceptable use agreements and children’s version of the internet safety policy*
* *contributing to online safety events with the wider school community e.g. parents’ evenings, family learning programmes etc.*

## Staff/volunteers

The DfE guidance “[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)” states:

“All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.”

“Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**”**

All staff will 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced.
* the training will be an integral part of the school’s annual safeguarding and data protection training for all staff
* all new staff will 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 includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
* the Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. LA / 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/INSET days
* the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

## Governors

Governors should take part in online safety training/awareness sessions, this may be offered in several ways such as:

* attendance at training provided by the local authority via Modern Governor
* participation in school training / information sessions for staff or parents

## Families

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 seek to provide information and awareness to parents and carers through:

* regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
* regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
* the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
* letters, newsletters, website, learning platform,
* high profile events / campaigns e.g. [Safer Internet Day](https://www.saferinternetday.org/)
* reference to the relevant web sites/publications, e.g. [SWGfL](https://swgfl.org.uk/audience/parents/); [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers)
* Sharing good practice with other schools in clusters and or the local authority

# Technology

The school is 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. This is managed and maintained by Virtue Technologies. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

## Filtering

* the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
* the school manages access to content across its systems for all users. The school uses Securus. The filtering provided meets the standards defined in the UK Safer Internet Centre
* access to online content and services is managed for all users
* illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
* there are established and effective routes for users to report inappropriate content
* there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
* *the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
* *younger learners will use child friendly/age-appropriate search engines e.g.* [*SWGfL Swiggle*](https://swiggle.org.uk/)
* filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
* *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
* *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](https://hwb.gov.wales/news/articles/0165ae84-0055-49b4-9bf2-0aedc29c5582) site.

## Monitoring

The DfE guidance “[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)” states:

“It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the … risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. “

The school has monitoring systems in place to protect the school, systems and users:

* The school monitors all network use across all its devices and services.
* An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. The Head Teacher is responsible for managing the monitoring strategy and processes.
* There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
* Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring) guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school’s risk assessment. These may include:

* physical monitoring (adult supervision in the classroom)
* internet use is logged, regularly monitored and reviewed
* filtering logs are regularly analysed and breaches are reported to senior leaders
* pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
* where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
* use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

## Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

* there will be regular reviews and audits of the safety and security of school technical systems
* servers, wireless systems and cabling are securely located and physical access restricted
* there are rigorous and verified back-up routines, including the keeping of network-separated in the cloud,
* all users have clearly defined access rights to school technical systems and devices.
* all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
* all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Virtue Technologies who will keep an up-to-date record of users and their usernames
* the master account passwords for the school systems are kept by Virtue Technologies
* The Head Teacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
* an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
* appropriate security measures are in place by Virtue Technologies to protect the servers, firewalls, routers, wireless systems and devices 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 workstations are protected by up-to-date endpoint (anti-virus) software.
* Temporary access of ‘guests’ is available, (e.g., trainee teachers, supply teachers, visitors) onto the school systems
* Users are unable to download executable files and installing programmes on school devices
* Removable devices are not permitted (e.g., memory sticks/CDs/DVDs) by users on school devices unless in exceptional circumstances with permission from the Head Teacher.
* systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

## Mobile technologies

The DfE guidance “Keeping Children Safe in Education” states:

*“The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 learning platform and other cloud-based services such as e-mail and data storage.

The school acceptable use agreements for staff, learners, and visitors outline the expectations around the use of mobile technologies.

The school allows:

|  |  |  |
| --- | --- | --- |
|  | **School devices** | **Personal devices** |
|  | School owned for individual use | 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 | Yes | Yes |
| Internet only | Yes | Yes | Yes | No | Yes | Yes |

## Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers’ professional conduct are set out in the [DfE Teachers Standards](https://www.gov.uk/government/publications/teachers-standards) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

* ensuring that personal information is not published
* education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
* clear reporting guidance, including responsibilities, procedures and sanctions
* risk assessment, including legal risk
* guidance for learners, parents/carers

School staff should ensure that:

* no reference should be made in social media to learners, 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
* security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
* they act as positive role models in their use of social media

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

* a process for approval by senior leaders
* clear processes for the administration, moderation, 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 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, 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 personal social media sites during school hours*

### Monitoring of public social media

* As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
* the school should effectively respond to social media comments made by others according to a defined policy or process
* when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by the Head Teacher to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the [Professionals Online Safety Helpline](https://saferinternet.org.uk/professionals-online-safety-helpline).

Alderley Edge Community Primary School has a separate Acceptable Use of Social Media Policy for the school community - <https://www.aecps.org/page/whole-school-community/113863>

## Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies**
* **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
* **staff/volunteers must be aware of those learners whose images must not be taken/published – lists available from the School Office**
* **Any images should only be taken on school devices.**
* in accordance with [guidance from the Information Commissioner’s Office](https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/taking-photographs-data-protection-advice-for-schools/), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, 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 school policies concerning the sharing, storage, distribution and publication of those images
* care should be taken when sharing digital/video images that learners are appropriately dressed
* 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 Online Safety Policy
* learners’ full names will not be used anywhere on a website or blog, particularly in association with photographs
* written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media
* parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy

## Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

* Public-facing website
* Social media
* Online newsletters

The school website is managed the Head Teacher and hosted by School Spider. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

## Data Protection

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

The school has a separate Data Protection Policy - <https://www.aecps.org/page/data-protection/113864>

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

* there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
* there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
* parents/carers are informed of patterns of online safety incidents as part of the school’s online safety awareness raising
* online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
* the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

### **Appendix**

The appendices are as follows:

A1 - Learner Acceptable Use Agreement Template

A2 - Staff (and Volunteer) Acceptable Use Policy Agreement Template

A3 - Community Users Acceptable Use Agreement Template

A4 - Responding to incidents of misuse – flow chart

A5 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A6 - Reporting Log

B1 - Training Needs Audit Log

 C1 - Links to other organisations and resources

Glossary of Terms

# School Online Safety Template Appendices

A1 Learner Acceptable Use Agreements Template

**Acceptable Use Policy for Early Years Pupils**

* I will take care when using the school IT equipment and use it properly.
* I will only share my username or password with trusted adults.
* I will tell an adult if I see anything which upsets me.
* I will use a safe name and not my real name on the internet.
* I will only take a photograph or video of someone if they say it is alright.
* Any messages I send will be polite.
* I will not deliberately write anything which upsets other people.
* I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment.
* I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name....................................................................................................

I confirm that I have read and understood this policy.

Signed....................................................................................

Relationship to child…………………………………………………………..

**Acceptable Use Policy for Key Stage 1 Pupils**

* I will look after all the school IT equipment and use it properly.
* I will only share my username or password with trusted adults.
* I will tell an adult if I see anything which upsets me.
* I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections.
* Any work I upload to the internet will be my own.
* I will only take a photograph or video of someone if they say it is alright.
* All of the messages I send will be polite.
* I will not post anything online which upsets other people.
* I will use a safe online name and not give away my personal information or talk to people I do not know using the internet.
* I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety.
* I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name....................................................................................................

I confirm that I have read and understood this policy.

Signed....................................................................................

Relationship to child…………………………………………………………..

**Acceptable Use Policy for Key Stage 2 Pupils**

* I will take care when using the school IT equipment and use it responsibly.
* I will keep my passwords private unless I need to share them with a trusted adult.
* I will inform an adult if I see or receive any unpleasant text, images or messages.
* I will not interfere with anyone else’s passwords, settings or files on the computer.
* I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
* Any work I upload to the internet will be my own.
* I know I need permission to take someone’s photograph or to video them.
* Any messages I post online or send in an email will be polite and responsible.
* I will not send or forward messages or create material which is deliberately intended to upset other people.
* I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.
* I will only bring my personal devices such as smart watches and mobile phones into school with the consent of my teacher. I will follow the school rules on storage of my devices during the school day.
* I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
* I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may happen even if the activity was done outside school.

Pupil name....................................................................................................

I confirm that I have read and understood this policy.

Signed....................................................................................

Relationship to child…………………………………………………………..

# A2 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 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 learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

### For my professional and personal safety:

* I understand that the school will monitor my use of the school digital technology and communications systems.
* I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, 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 systems:

* I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
* I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (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 only use social networking sites in school in accordance with the school’s social medial policy.
* I will only communicate with learners 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 has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

* When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
* I will not use personal email addresses on the school’s ICT systems.
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will ensure that my data is regularly backed up, in accordance with relevant school policies.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
* I will not disable or cause any damage to school 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 Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
* I understand that data protection policy requires that any staff or learner 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 online systems 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’s digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
* I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. (See Staff Disciplinary Policy)

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:

# A4 Acceptable Use Agreement for Community Users Template

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

* that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
* that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that users are protected from potential harm in their use of these systems and devices

### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

* I understand that my use of school systems and devices will be monitored
* I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

* I will not access, copy, remove or otherwise alter any other user’s files, without permission.
* I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
* I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
* I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I will immediately report any damage or faults involving equipment or software, whatever the cause.
* 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 if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school 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.

|  |  |
| --- | --- |
| **Who will have access to this form.**The School Office and Head Teacher | **How this form will be destroyed.**Deleted/shredded when no longer in school |
| **Where this form will be stored.**School office | **How long this form will be stored for.**Only whilst accessing school  |

Name: Signed: Date:……………………………………….

# A5 Responding to incidents of misuse – flow chart



# A6 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

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

|  |
| --- |
| A7 Reporting LogGroup:  |
| Date | Time | Incident | Action Taken | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| B1 Training Needs Audit LogGroup:  |
| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## C1 Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - h[ttps://swgfl.org.uk/products-services/online-safety/](http://www.swgfl.org.uk/)

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

Harmful Sexual [Support](https://swgfl.org.uk/harmful-sexual-behaviour-support-service/) Service

### CEOP

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](http://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

### Others

[LGfL – Online Safety Resources](https://www.lgfl.net/online-safety/resource-centre?a=3)

[Kent – Online Safety Resources page](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

### Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk/)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups](http://www.360groups.org.uk/) – online safety self review tool for organisations working with children

[SWGfL 360 Early Years](http://www.360earlyyears.org.uk/) - online safety self review tool for early years organisations

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - [https://selma.swgfl.co.uk](https://selma.swgfl.co.uk/)

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance - <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf>

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](http://www.childnet.com/our-projects/project-deshame)

[UKSIC – Sexting Resources](https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/teaching-resources/sexting-resources)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](https://www.ditchthelabel.org/)

[Diana Award – Anti-Bullying Campaign](http://www.antibullyingpro.com/)

### Social Networking

Digizen – [Social Networking](http://digizen.org/socialnetworking/)

UKSIC - [Safety Features on Social Networks](https://saferinternet.org.uk/guide-and-resource/social-media-guides)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](https://www.tes.com/teaching-resources/digital-citizenship)

### Curriculum

53

SWGfL Evolve - [https://projectevolve.co.uk](https://projectevolve.co.uk/)

[UKCCIS – Education for a connected world framework](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis)

[Department for Education: Teaching Online Safety in Schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.de/en/)

Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

### Data Protection

[360data - free questionnaire and data protection self review tool](http://360data.org.uk/)

[ICO Guides for Organisations](https://ico.org.uk/for-organisations/%22%20%5Ct%20%22_blank)

[IRMS - Records Management Toolkit for Schools](https://irms.org.uk/general/custom.asp?page=SchoolsToolkit" \t "_blank)

[ICO Guidance on taking photos in schools](https://ico.org.uk/for-the-public/schools/photos/)

### Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2)

[Childnet – School Pack for Online Safety Awareness](http://www.childnet.com/resources/school-pack-for-online-safety-awareness)

[UK Safer Internet Centre Professionals Online Safety Helpline](http://www.saferinternet.org.uk/helpline)

### Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)

SWGfL Safety & [Security](https://swgfl.org.uk/resources/) Resources

Somerset - [Questions for Technical Support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)

SWGfL - [Cyber Security in Schools](https://swgfl.org.uk/research/cyber-security-in-uk-schools/).

NCA – [Guide to the Computer Misuse Act](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file)

NEN –  [Advice and Guidance Notes](https://www.nen.gov.uk/advice/%22%20%5Ct%20%22_blank)

###

### Working with parents and carers

SWGfL – Online Safety Guidance [for](https://swgfl.org.uk/resources/online-safety-guidance-for-parents/) Parents & Carers

[Vodafone Digital Parents Magazine](http://www.vodafone.com/content/parents/digital-parenting.html)

[Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers)

[Get Safe Online - resources for parents](https://www.getsafeonline.org/personal/article-category/safeguarding-children/%22%20%5Ct%20%22_blank)

[Teach Today - resources for parents workshops/education](http://www.teachtoday.de/en/%22%20%5Ct%20%22_blank)

[Internet Matters](https://www.internetmatters.org/)

### Prevent

[Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance)

[Prevent for schools – teaching resources](http://www.preventforschools.org/)

Childnet – [Trust Me](https://www.childnet.com/resources/trust-me)

### Research

[Ofcom –Media Literacy Research](https://www.ofcom.org.uk/research-and-data/media-literacy-research)

[Ofsted: Review of sexual abuse in schools and colleges](https://www.gov.uk/government/publications/review-of-sexual-abuse-in-schools-and-colleges/review-of-sexual-abuse-in-schools-and-colleges)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

## Glossary of Terms

**AUP/AUA** Acceptable Use Policy/Agreement – see templates earlier in this document

**CEOP** Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

**CPD** Continuous Professional Development

**FOSI** Family Online Safety Institute

**ICO** Information Commissioners Office

**ICT** Information and Communications Technology

**INSET** In Service Education and Training

**IP address** The label that identifies each computer to other computers using the IP (internet protocol)

**ISP** Internet Service Provider

**ISPA** Internet Service Providers’ Association

**IWF** Internet Watch Foundation

**LA** Local Authority

**LAN** Local Area Network

**MAT** Multi Academy Trust

**MIS** Management Information System

**NEN** National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

55

**Ofcom** Office of Communications (Independent communications sector regulator)

**SWGfL** South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

**TUK** Think U Know – educational online safety programmes for schools, young people and parents.

**UKSIC** UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

**UKCIS** UK Council for Internet Safety

**VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

**WAP** Wireless Application Protocol

56

54

57

1. In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient ‘separation of responsibility’ should this be the case. [↑](#footnote-ref-1)
2. See flow chart on dealing with online safety incidents in ‘[Responding to incidents of misuse’](#_Reporting_and_responding) and relevant local authority/MAT/ HR/other relevant body disciplinary procedures. [↑](#footnote-ref-2)