The Aspire Federation

Being a Good Digital Citizen

New technologies have become integral to the lives of learners and young people today, both within school and in their lives outside of school.

The internet, other forms of digital communication and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps us learn from each other. These technologies can stimulate discussion, promote creativity and effective learning. At Aspire we believe that everyone has an entitlement to safe internet access at all times.

Aim

- Our aim is to ensure that learners can use digital communication and information technologies appropriately and safely as part of our wider duty of care.

Intentions

- We intend to build learner resilience, confidence and the skills to face and deal with risks to which they may be exposed.

These risks may include;

- Access to illegal, harmful or inappropriate images or other content,
- Unauthorised access to/loss of/sharing of personal information. The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers,
- Cyber-bullying,
- Access to unsuitable video/internet games,
- The evaluation of the quality, accuracy and relevance of information on the internet,
- Plagiarism and copyright infringement,
- Illegal downloading of music or video files,
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person.

Responsibilities

Governors

It is the responsibility of the Governing Body to bi-annually approve and review the effectiveness of the Being a Good Digital Citizen policy.

At Aspire we have a Digital Citizen Governor, whose role includes;

- Meeting with the Digital Citizen Council,
- Monitoring of e-safety incident logs,
- Reporting to the Governing Body.

Governors are required to fully comply with this policy and the data protection policy in the event they have access to personal data.

Strategic Leads

It is the responsibility of the Strategic Alliance Team, Strategic Development Manager and Data Protection Officer to;

- Review, monitor and evaluate all aspects of e-safety within the context of whole school self-evaluation and development planning,
- Ensure staff receive relevant CPD,
- Ensure that there is a system in place, as a 'safety net' to monitor daily e-safety issues,
- Ensure procedures are followed in the event of a serious e-safety allegation being made against a member of staff, (see flow chart p7)
- Feedback to the Governing Body through the Head of School's Report,
- Keep up to date with current legislation and guidance,
- Determine and take responsibility for the school's information risk policy and risk assessment,
- Determine who has access to; protected data and why, how long information is stored for, the method of storage, how it is added to or amended.
- Authorise appropriate access data held by school in compliance with DPA 2018, retention policy and DPP.

Senior Leadership Team

It is the responsibility of the Senior Leadership Team to;

- Review and analyse monitoring reports from Technical Support,
- Provide all new staff with e-safety training as part of their induction programme, ensuring that they fully understand the school's 'Being a Good Digital Citizen' policy.

Strategic Technical Development Officer/Technical Support

It is the responsibility of the Strategic Technical Development Officer/Technical Support to;

- Protect School's ICT infrastructure from misuse or malicious attack,
- Ensure that School meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety policy and guidance,
- Receive reports of e-safety incidents and creates a log of incidents,
- Use remote management tools to control workstations and view user's activity, where appropriate,
- Have a leading role in establishing and reviewing our Being a Good Digital Citizen policy and associated documents,
- Ensure School uses filtering software on its servers and updates them on a regular basis,
- Implement monitoring software/systems and keep them updated as detailed in school policies,
- Ensure there will be regular reviews and audits of the safety and security of School ICT systems,
- Ensure servers and cabinets are securely located and physical access restricted,
- Regularly monitor the use of devices connected to our networks in order that any misuse/attempted misuse can be reported to the Senior Lead,

- Make available to the Head of School the master/administrator passwords for the school ICT system, used by the Strategic Technical Development Officer. These should be kept in a secure place (e.g. school safe).

All Staff

It is the responsibility of all staff to;

- Encourage a focus on e-safety in all areas of the curriculum. Being a Good Digital Citizen Charter as a code of conduct.
- Inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images; in particular, recognising the risks attached to publishing their own images on the internet e.g. on social networking sites,
- Use personal data in accordance with data protection policy and this policy. Access personal data using school provided devices, using secure passwords and ensuring that they are properly "logged-off" at the end of any session in which they are using personal data,
- Ensure that PCs they are using are 'locked' when left temporarily unattended.
- Transfer data using encryption and secure password protected devices. ***Please note that if passwords are lost data cannot be retrieved from encrypted devices.***
- Ensure any school owned devices used are kept up to date by technicians.
- Devices and/or removable media that have become damaged should be handed back to Tech Support to be disposed of securely to avoid data leakage.

Learners

It is the responsibility of all learners to;

- Use schools' ICT systems in accordance with the Being a Good Digital Citizen Charter,
- Sign the Being a Good Digital Citizen Charter before being given access to school systems,
- Report abuse, misuse or access to inappropriate materials,
- Consider plagiarism and value copyright regulations when accessing the internet.

Parents and Carers

Parents /Carers play a crucial role in ensuring that young people understand the need to use digital communication and information technologies in an appropriate way. Parents and carers can;

- Access a copy of the full policy on the school websites.
- Annually receive the Being a Good Digital Citizen Charter to share with their son/daughter. **(Appendix 1)**

Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.

Procedure and practice

Learning

- A planned e-safety programme should be provided as part of ICT/PHSE and other relevant curricular areas and should be regularly revisited to cover both the use of ICT and new technologies in school and outside school,
- Key e-safety messages should be reinforced as part of a planned programme of assemblies, form time activities and event days,
- Learners should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information,
- Being a Good Digital Citizen Charter is displayed in all rooms and on the log in screens,
- Staff should act as good role models in their use of digital communication and information technologies.

Monitoring and review

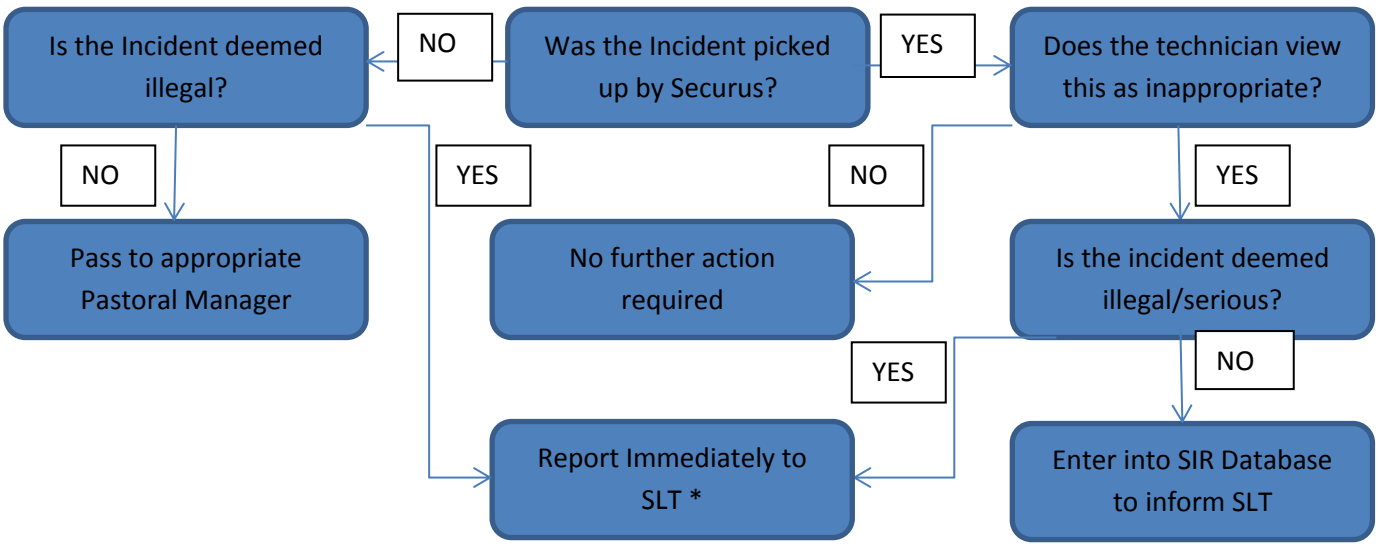
At Aspire we use software to monitor inappropriate ICT usage.

The monitoring software which identifies cyber bullying and other safeguarding concerns. It monitors learners and staff when they use ICT and captures e-safety risks that would otherwise go undetected. The software identifies issues by analysing text and images displayed on all computer screens. The software captures evidence of every incident and alerts School if the situation is serious or urgent. Logs are reviewed on a daily basis and any inappropriate findings are passed on to the appropriate Senior Lead.

Responding to incidents of misuse

All members of the school community should be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse. The flow chart below lists the responses that will be made to any apparent or actual incidents of misuse that appear to involve illegal activity, i.e. material which potentially breaches the Obscene Publications Act, criminally racist material and other criminal conduct, activity or materials.

E-safety Serious Incident Flow Chart



* SLT to report illegal incidents to the police, ensuring the preservation of evidence.

Investigation of Complaints

The School will investigate complaints received from both internal and external sources, about any unacceptable use of Aspire digital communication and information systems.

The investigation of facts of a technical nature will be undertaken by the Systems Manager or/and any 3rd parties, i.e. the Head of School, or/and the LA.

If any suspected or confirmed misuse takes place involving personal data this should be reported to the DPO who will investigate.

Where there is evidence of a criminal offence, the issue will be reported to the police for them to take appropriate action. The School will co-operate with the police and other appropriate external agencies in the investigation of alleged offences.

Filtering

Software used at Aspire for filtering includes Smoothwall. At least one of these will be used at each school. Aspire works with the Local Authority and the Internet Service Provider to ensure that systems to protect learners are regularly reviewed and improved. If staff or learners discover unsuitable sites, the URL (Uniform Resource Locators) must be reported to the Technical Support Team via the helpdesk.

A key feature of the filtering software is the ability to categorise websites and then allow or restrict users' access by selecting categories. Examples of the categories are: Adult/Sexually Explicit, Advertisements, Popups, Personal, Dating, Proxies and Translators.

The supplying company updates its database of sites and categories daily and the update is provided to school. The school filtering software provides a further layer of protection. The Systems Manager, at regular intervals, monitors the list of recently visited URLs and in real time whilst learners are working.

Internet Access to Materials of an Extreme Nature.

The Aspire Federations' computers are monitored through the SECURUS internet monitoring system. The system is used to restrict access to known sites relating to the Safeguarding of Children and Young People. The system records details relating to site access, keyword searches and it is possible to produce screen images showing the type and nature of material accessed.
In line with the federation's safeguarding procedures any evidence of key word searches or access to inappropriate sites identified by SECURUS will trigger a referral to the designated safeguarding lead in each school, who will follow the relevant safeguarding policy and make appropriate professional referrals.

Acceptable Use

Users are responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security. This should be reported to the technician's team and DPO.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action. Particularly, all transfer of data is subject to risk of loss or contamination.

Processing and transmission of information which contains personal data about individuals requires proper legal justification under the DPA 2018 & GDPR. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal.

Any purchase of systems that process information for us (eg. Earwig) must be begun in consultation with the DPO, who will ensure that we comply with current laws.

Requests from staff for sites to be removed from the filtered list will be considered by the Strategic Technical Manager. If the request is agreed, this action will be recorded, and logs of such actions shall be kept.

Temporary network access for visitors and trainee teachers is allowed through guest accounts which are enabled for the duration of the visit. By using the guest accounts visitors agree to the terms and conditions of this policy.

Staff and learners are not allowed to install programmes or executable files on workstations or portable devices. Should a piece of software or app needs installing then a request via the helpdesk should be made.

Any attempts to breach firewalls will result in a ban from using school ICT equipment without close supervision.

Staff access to the internet and email is on the clear understanding that any misuse will be taken seriously, and disciplinary action may result, and dismissal may follow. 'Misuse' includes;

- Accessing, displaying, downloading or disseminating pornographic or other 'adult' materials,
- Editing any personal information without proper authorisation
- Viewing or using personal information in a way that does not contribute to carrying out their regular duties.
- Posting information that may tend to disparage or harass others based on gender, race, age, disability, religion, sexual orientation, political affiliation or national origin,
- Publishing information that is false, misleading or defamatory concerning the school or Local Authority or any other company, organisation or individual that could bring the school or Local Authority into disrepute,
- Participating in any form of gambling,
- The transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind or the unauthorised transmission to a third party of confidential material concerning the activities of the Aspire Federation,
- Sharing of private email conversations with others without the author's consent.

Personal Use of Email

Aspire permits the use of its IT facilities for email by learners, staff and other authorised users for personal use, subject to the following limitations;

- A level of use that is reasonable and not detrimental to the main purpose for which the email service is provided,
- Priority must be given to use of resources for the main purpose for which they are provided,
- Personal use must not be connected to any purpose or application that conflicts with the School's rules, regulations, policies and procedures,
- If users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance from Tech Support, in the case of learners, their teacher.

SLT will exercise discretion in judging reasonable bounds within the above standards for acceptability of material transmitted by email.

Social Networking

See **the Aspire Federation's Social Media Policy**

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by Aspire or by a third party) must be approved by the Head of School.

The Terms of Use in the Social Media Policy apply to all uses of social networking applications by all school representatives.

We expect that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and ensuring lawful conduct.

Parents and carers will be asked to complete a Social Media Consent Form for any use of image, video, work or name (See **Appendix 2**)

Hardware

We take pride in our extensive range of ICT equipment. To keep this equipment in the best working order, staff and learners must ensure that they do not misuse any hardware equipment.

- Resources must not be used for commercial purposes or monetary gain.
- Aspire reserves the right to hold you financially liable if, through negligence or deliberate action, resources are compromised in any way.
- All staff need to ensure that their portable devices are available for regular checks when requested annually for audit.
- All ICT equipment must be bar-coded and put into the asset management database. All ICT equipment must be security marked before deployment.
- Appropriate security measures are in place to protect the servers, firewalls,

routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

Purchase of ICT equipment

- Any subject leader or budget holder wishing to purchase ICT hardware or software should contact the Technical Support Team, who will find the supplier offering the best value. This may involve a bidding process for larger orders.

Ownership/management of ICT equipment

- Portable ICT equipment will be stored and managed centrally by the technical team. The team will be responsible for stock control of this equipment.
- Booking of portable equipment should be made via the helpdesk giving 24 hours' notice, equipment is assigned to staff for the borrowing period via the asset management software.
- Fixed hardware should only be moved by the Technical Support by request via the helpdesk.

Data Handling and removable media

It is the responsibility of all members of the school community to ensure the safety and security of any material of a personal or sensitive nature. It cannot be accessed by anyone who does not either have permission to access or a need to have access to the data. This includes; research data, teaching and learning data, administration and management information data e.g. sims).

For the purposes of this policy, all data is fairly obtained, lawfully processed and categorised in line with the Data Protection Act (DPA) 1998, 2018 and the General Data Protection Regulation (GDPR).

Personal Data

For full detail on the data we collect and use, please see the privacy notice on our websites.

School will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any data items that could be used to identify a living individual. Personal data can provide specific information about an individual, their families or circumstances. This will include;

- Personal information about members of the school community - including learners, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records, photographs.
- Curricular/academic data e.g. class lists, learner progress records, reports, references, exam results.
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references,

- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Special Category Data Special category data includes any data identified by the Data Protection Act (2018) and the GDPR as special category data, specifically data relating to:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- membership of trade union organisations,
- physical or mental health,
- sexuality and sex life,
- offences or alleged offences,
- Biometric information e.g. fingerprint.

Registration

Each school within Aspire is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Training & awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Audit/training at September Inset,
- Induction training for new staff and trainee teachers including audit and risk assessment,
- Staff meetings/briefings/Inset.

Secure storage of and access to data

School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All portable and removable media/storage devices must be encrypted and stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

All data stored on the servers will be backed up and a copy stored off site. See Data Backup policy for further details.

Disposal of data

We will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other media must be shredded, incinerated or otherwise disintegrated for data.

Disclaimers

School may arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the Aspire Federation, in order to provide necessary legal protection.

School copyright policy

School will respect all copyright rights including:

- the rights of owners of third-party material used in teaching,
- the rights of learners in all material they create in and for school,
- the rights teachers have in material they created prior to being employed at the Aspire federation and in material created while employed at school.

We will comply with UK copyright legislation including sections relating to educational and library use.

We will purchase appropriate copyright licences where its use of copyright material exceeds that permitted under the Act and the schools will comply with the terms of these licences.

While acknowledging that we cannot control all actions of our learners, the schools will endeavour to educate learners and staff on copyright use, including referencing, approved copying, and proper use of electronic material and downloadable music.

Other relevant policies to be read in conjunction;

Respect Charter (Anti-bullying Policy), Behaviour for Learning policy, Systems Management policy, Safeguarding and Child Protection policy, Data Backup Policy, Data Protection Policy & Privacy Notice, Social Media Policy, Radicalisation and Extremism Policy, Whistleblowing policy, Staff Behaviour policy, Induction policy.

Date approved	**08.01.2021**
Review Date:	**December 2022**
Signed Executive Headteacher:	**C Taylor**
Chair of Governors	**J Brown**

Appendix 1

Being a Good Digital Citizen Charter

I will use the school network and technology responsibly and respectfully at all time.

- I will only use my own user name and password and keep them secret.
- I will only access websites that my teacher has approved.
- I will report any accidental damage immediately to the staff
- I will report any messages I see that make me feel uncomfortable.
- I will not delete or change another person's work.
- I will not download software, games or videos
- I will not damage any computer equipment or the school network in any way.
- I will not send nasty messages to anyone
- I will not give out personal information including addresses, telephone.

I understand that the school can check my computer files, and the Internet sites I visit and that if they have any concerns about my safety, that they may contact my parent / carer.

I understand that if I do not follow these rules, I will be denied access to the computer network for a time to be determined by the Head of School and may face further disciplinary action depending on the nature of the offence.

Year Group / Class: _____

Learner

I agree to follow the school's Acceptable Use Policy on the use of the technology. I will use the technology in a responsible way and obey all the rules explained to me by the school.

Learner Signature: _____ Date: _____

Appendix 2

The Aspire Federation

PHOTOGRAPH/PUBLICITY/SOCIAL MEDIA
PARENT/GUARDIAN CONSENT FORM

Please read the following agreement carefully.

Social media can offer a variety of benefits without risking any safety to learners or members of the school community. It is an excellent opportunity for school/college to connect with families and share information about school events and activities. (school name) uses Facebook, Twitter and You Tube.

Please tick to indicate your consent to photographs/videos of your child being used in the stated ways below. This agreement will continue throughout your son/daughter's time at (school name). If at any time you wish to withdraw your consent, please inform the school in writing.

As the named parent/carer of: …….. Year / Class……

I hereby agree to photographs/videos of my child being used in the following ways.

	Please tick
I am happy for my child's photograph to be used and displayed within school.	
I am happy for video footage of my child to be used within school.	
I am happy for video footage of my child during school productions/events to be sent out to other Parents of the school.	
I am happy for my child's photograph to be used in publicity including press photographs, interviews and videos. (these may be used outside of school)	
I am happy for my child's photograph to be used in school newsletters. (newsletters are sent out to all learners and staff)	
I am happy for my child's photograph to be used on the Aspire/(school name) websites and on (school name)'s social media sites	
I am happy for videos of my child to be used on the Aspire/(school name) websites and on (school name)'s social media sites	
I am happy for my child's school work to be shared on (school name)'s social media sites	
I am happy for photographs/videos of my child to be shared with other schools/professional bodies on their social media sites	
I am happy for my child's first name to be shared on social media sites (please note the school will not share the surname of any learner on social media sites)	
I am **NOT** happy for photographs of my child to be used in any way except those related to evidence of their school work	
I am **NOT** happy for videos of my child to be used in any way except those related to evidence of their school work	

Signed……Date……