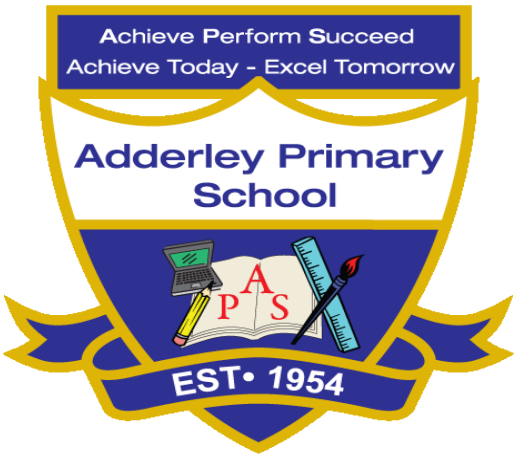


E-Safety Policy

2018 - 2020

Agreed by:	Governing Body	
Review date:	November 2020	

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.
While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- 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
- An inability to evaluate 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 social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents/carers and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.
It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT
E-Safety is led by the Strategic Leadership team and Network Manager who meets on a weekly basis to

- Review and monitor any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as Children's Services, the Police, the Child Exploitation and Online Protection Centre (CEOP) and the Birmingham Local Authority ICT service provider – Link2ICT.

Responsibilities of Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. Governors will;

- Request regular feedback from the SLT on the effectiveness of the E-Safety policy
- Monitoring e-safety incident logs and challenge leaders as to the effectiveness of action taken
- Monitoring of filtering and hold SLT to account for their actions
- Monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices
- Ensure that the school involves the appropriate agencies if criminal material is discovered

Responsibilities of the Head Teacher

The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the SLT. The Head Teacher will;

- Ensure procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents)
- Ensure relevant disciplinary procedures are followed in the event of serious incidents occurring
- Ensure that the relevant outside agencies are contacted in relation to the nature of the material discovered or the event which has occurred

Responsibilities of the Strategic Leadership Team (SLT)

Our SLT is the responsible to the Head Teacher and governors for day to day issues relating to e-safety. They will;

- Receive notifications from the school's computer monitoring software (Policy Central) and take day-to-day responsibility for e-safety issues
- Report regularly to the Head Teacher
- Review the school e-safety policies / documents in line with new guidance and technology
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Provide training and advice for staff and induct new staff on the acceptable use of ICT
- Liaise with the Local Authority and other agencies as necessary
- Liaise with school Network Manager
- Attend relevant meetings and committees of the Governing Body and report incident logs and action taken
- Receive appropriate training and support to fulfil their role effectively
- Have responsibility for directing the Network Manager to blocking / unblocking internet sites or users with the school's filtering system
- Maintain detailed logs of any occasions where the school has used its powers of search and deletion of electronic devices

Responsibilities of the Network Manager and ICT technician(s)

The Network Manager and ICT Technician(s) are responsible for ensuring that;

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack

- Users may only access the school's networks through properly enforced password protection
- Shortcomings in the infrastructure are reported to the SLT or Head Teacher so that appropriate action may be taken

Responsibilities of All Staff

Teaching and Support Staff are responsible for ensuring that;

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and accepted the school's Acceptable Use Policy for staff
- They report any suspected misuse or problem to the SLT
- Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems and with the full consent and awareness of the SLT and Head
- E-safety issues are embedded in the curriculum and other school activities

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the SLT under the direction of the Head Teacher. Monitoring will take place at regular intervals by the Governing Body who will receive a report on the implementation of the e-safety policy will include anonymous details of e-safety incidents.

The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the Acceptable Use of Technologies Policy, which they will be expected to sign before being given access to school systems.

The Acceptable Use of Technologies Policy is provided in Appendix 1 of this policy for:
Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time.

Parents sign once when their child enters the school for permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work. A copy of the pupil AUP is also made available to parents at via the website.

Staff and pupils also accept the policy every time they log on to computer equipment at school. Induction policies for all members of the school include this guidance.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

Type of inappropriate activity	**External Agencies to Involve/Policies to Consult**
Child sexual abuse images (**illegal** - The Protection of Children Act 1978)	• Police • School disciplinary procedures (if staff) • Birmingham Safeguarding Children's Board • Children's Services
Grooming, incitement, 'sexting', arrangement or facilitation of sexual acts against children (**illegal** – Sexual Offences Act 2003)	• Police • School disciplinary procedures (if staff) • Birmingham Safeguarding Children's Board • Children's Services
Possession of extreme pornographic images (**illegal** – Criminal Justice and Immigration Act 2008)	• Police • School disciplinary procedures (if staff)
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (**illegal** – Public Order Act 1986)	• Police • School disciplinary procedures (if staff) • Prevent • Counter Terrorism Unit
Pornography – any form of nudity or sexually suggestive materials	• Behaviour policy • School disciplinary procedures (if staff)
Promotion of any kind of discrimination (possibly a breach of The Equality Act 2010)	• Behaviour policy • Consult Equality Policy and guidance • School disciplinary procedures (if staff)
Promotion of racial or religious hatred, radicalisation and/or extremism (**illegal** - Racial and Religious Hatred Act 2006)	• Behaviour policy • Police • Prevent • Counter Terrorism Unit School disciplinary procedures (if staff)
Threatening behaviour, including promotion of physical violence or mental harm (**potentially illegal**)	• Behaviour policy • Police advice should be sought • School disciplinary procedures (if staff)
Any other information which may be offensive to children/colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	• Behaviour policy • School disciplinary procedures (if staff)

Additionally the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards

- employed by the school and/or Local Authority
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil sanctions

	Refer to class teacher	Refer to SLT	Refer to Head Teacher	Refer to Police – or other agencies	Inform parents / Carers	Removal of network / internet access	Warning/Behaviour policy sanctions	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔	✔			✔	✔	✔	
Unauthorised use of mobile phone / digital camera / other handheld device	✔	✔			✔	✔	✔	
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔	✔	
Unauthorised downloading or uploading of files	✔	✔			✔	✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔	✔	✔	✔
Attempting to access the school network, using another pupil's account	✔	✔			✔	✔	✔	
Attempting to access or accessing the school network, using the account of a member of staff	✔	✔	✔		✔	✔	✔	✔
Corrupting or destroying the data of other users	✔	✔			✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔	✔	✔	✔	✔	✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔	✔		✔	✔	✔	✔
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔	✔		✔	✔	✔	
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔	✔	✔	✔	✔	✔
Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulations	✔	✔	✔		✔	✔	✔	

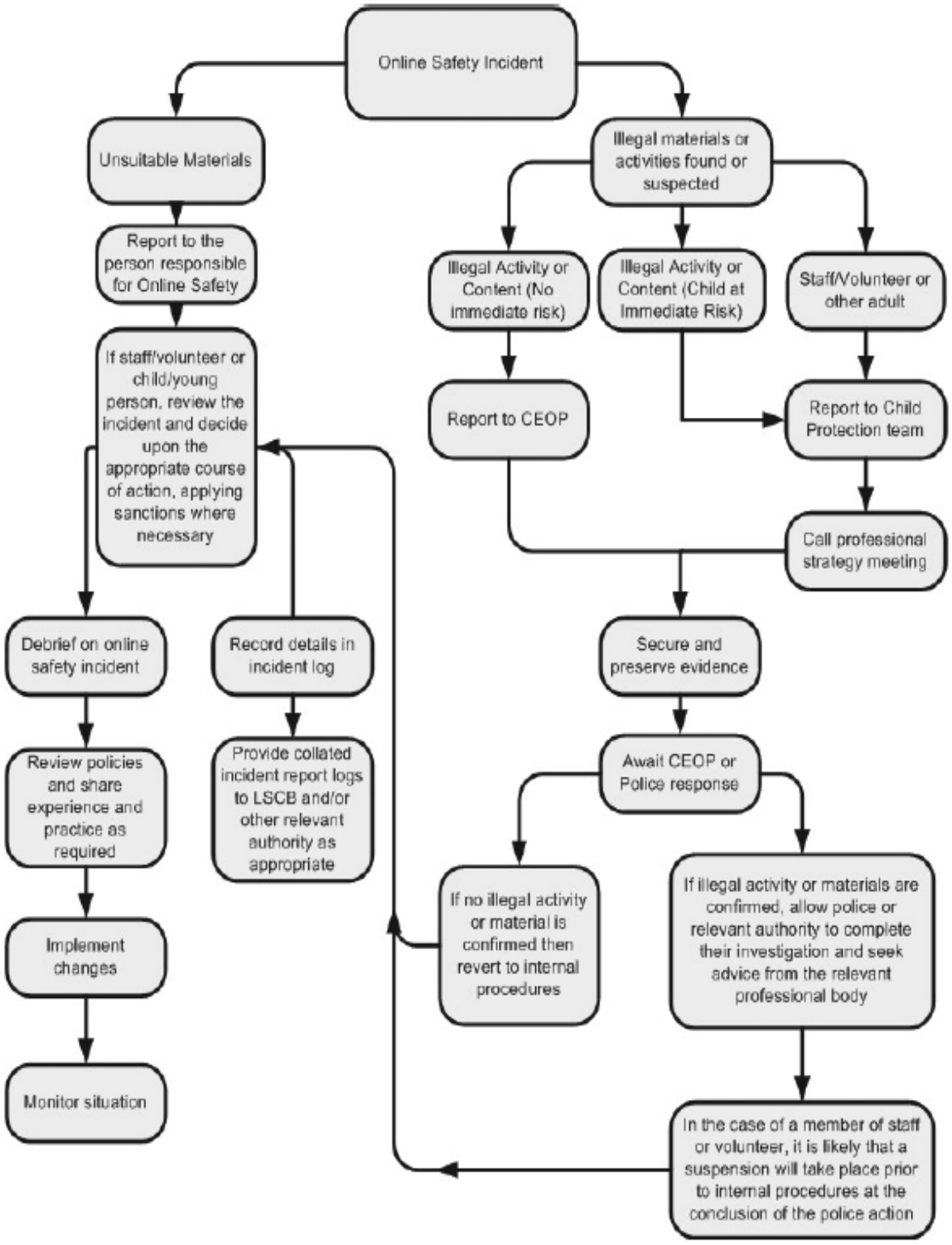
Staff sanctions

	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Code of conduct warning	Disciplinary action/Suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	✔	✔	✔	✔	✔	✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔			✔	✔	
Unauthorised downloading or uploading of files	✔	✔			✔	✔	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔	✔				✔	
Careless use of personal data eg holding or transferring data in an insecure manner	✔	✔			✔	✔	✔
Deliberate actions to breach GDPR or network security rules	✔	✔			✔	✔	✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔	✔	✔			✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔			✔	✔
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✔	✔	✔			✔	✔
Actions which could compromise the staff member's professional standing	✔	✔	✔			✔	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔	✔			✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔			✔	✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔	✔		✔	✔	✔
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔
Breaching copyright or licensing regulations	✔	✔			✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔		✔	✔	✔

Reporting e-safety breaches

It is hoped that all members of the school community will 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 or irresponsible or, very rarely, through deliberate misuse. This flow chart shows the process that should be followed.

All misuse must be reported to a member of the SLT as soon as possible.



Managing E-Safety Breaches

This guidance is intended for use by Senior Leaders when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse)
- 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 disciplinary procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include;

  incidents of 'grooming' behaviour
  the sending of obscene materials to a child

Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.
Record the incident and actions taken on a 'Policy Central Form' and retain for evidence and reference purposes.

Audit / Monitoring / Reporting / Review

Mobile phones are not allowed in school. However, children may bring in handheld devices such as iPads on special days. The SLT will ensure that full records are kept of incidents involving the

searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by the Head Teacher / and Governors on a termly basis.

Use of hand held technology (personal phones and hand held devices)

(Refer to Mobile Phone and Cameras Policy)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is as follows;

- Members of staff are permitted to bring their personal mobile devices into school.
- They must only use them as directed in the **Staff Handbook** and **Mobile Phones Policy**.
- Pupils are not currently permitted to bring personal hand held devices into school.
- A number of such devices are available in school (e.g. iPads, Kindles, ActiVote) and are used by children as considered appropriate by members of staff. Use of these devices is only permitted under supervision of permanent staff members.

Use of digital and video images

(Refer to Mobile Phone and Cameras Policy)

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Members of staff are allowed to take digital still and video images to support educational aims, but must;

- ensure the child(ren) being photographed have parental consent for images to be taken
- follow school policies concerning the sharing, distribution and publication of those images.
- only captured images using school equipment; the personal equipment of staff should not be used for such purposes
- take care when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- not take, use, share, publish or distribute images of others without permission from the Head Teacher
- See also the following section for guidance on publication of photographs

Email

Access to email is provided for all users in school via Office 365 email suite provided by the City Council internet service provider, Link2ICT.
These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access)
- Staff **MUST NOT** communicate with pupils or ex-pupils by email
- Staff should inform the SLT if any pupil attempts to make contact with them via email
- Pupils are informed that they must not attempt to communicate with staff by email
- Staff must not access personal email accounts whilst at school or on school equipment.
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school

- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
- Users must immediately report, to the SLT any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of web-based publication tools

Our school uses the public facing website, www.adderleyprimary.co.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.
Currently only the SLT (and the Network Manager – with SLT permission) can publish information on the website.

- Personal information should not be posted on the school website including official email addresses of staff and pupils
- Only pupil's first names are used on the website, and only then when necessary
- Only calendars of school events relevant to parents/carers are published on the school website
- Staff must pay due regard to child protection and safeguarding matters before publishing pupil details online. They should seek advice from other DSLs if unsure.
- Pupil photographs can only be published online if permission from parent/carer has been received by school. There is no assumed consent where consent has not been received.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images;

Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs, class names etc. Pupil first name and year group is acceptable.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Use of USB/removable devices and/or file sharing websites
(Refer to Mobile Phone and Cameras Policy)

Only USB/removable devices which are suitably encrypted can be used by staff. All staff laptops are secured with password protection.

File sharing and cloud storage websites (other than the school's own Dropbox account) should not be accessed by staff on school equipment.

Use of and access to Social Media

All known social media sites are blocked by the school's filtering system. New or previously unknown social media sites can be blocked by the school as they arise. Staff should not attempt to access social media sites via school equipment at any time.

The school utilises a Twitter account in order to inform parents/the community of school matters. The password for this account is only known to the SLT. Any tweets or communications can only be sent by an SLT member with the permission of the Head Teacher.

Staff should be aware of the following legal risks surrounding their use off social media which can lead to disciplinary action;

- Posting or contributing to derogatory comments about the school (this may including indicating 'liking' a derogatory comment
- Posting pictures/video clips on social media which may bring the school in to disrepute
- Leaking confidential material/information about the school via social media
- Airing controversial views (including views not in keeping with fundamental British values) using social media/blogs
- Posting content which is subject to copyright or is inaccurate
- Accessing or attempting to access social media sites on school equipment
- Cyberbullying, harassment or maltreatment of others via social media

Internet Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.
As a school buying internet access, email and technical support services from Birmingham's 'Link2ICT' Services we automatically receive the benefits of a managed filtering service using a program called 'Policy Central', with some flexibility for changes at school level.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the SLT (with ultimate responsibility resting with the Head Teacher and Governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.
To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Link2ICT filtering service must:

- Be authorised by more than one responsible person in case there is a breach by one of the responsible persons
- Be kept up-to-date with filtering issues that arise
- Be monitored and set to send out alerts to the SLT

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.
Staff users will be made aware of the filtering systems through:

- The school induction process
- In Service Training (INSET)

- Briefing in staff meetings, training days etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through safety awareness information in the newsletter etc.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Any breaches will be recorded in the 'Policy Central' folder (kept by the Head Teacher) along with the action which was taken in response to the breach. This folder is available to be scrutinised by Governors and other agencies as appropriate.

E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's safety provision. Children and young people need the help and support of the school to recognise and avoid safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.
E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Pupils are **NEVER** allowed to use ICT equipment unsupervised
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education
- http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber CafJ at KS2)
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils take part in Safer Internet Day each year
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

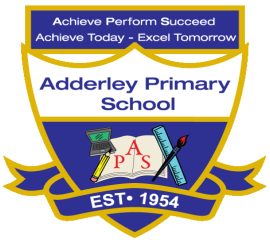
  Checking the likely validity of the URL (web address)
  Cross checking references (can they find the same information on other sites)
  Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils are taught how to make best use of internet search engines to arrive at the information they require

We use the resources on CEOP's Think U Know site as a basis for our e-safety education

Documents and relevant legislation

E-Safety Model Policy Birmingham City Council 2014
Education Act 1996
Education and Inspections Act 2006
Education Act 2011 Part 2 (Discipline)
The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
Health and Safety at Work etc. Act 1974
Obscene Publications Act 1959
Children Act 1989
Human Rights Act 1998
Computer Misuse Act 1990
This is not a full list of Acts involved in the formation of this advice. Further information about relevant



POLICY CENTRAL INCIDENT FORM (E-SAFETY)

Name:	**Date:**
Class:	**Place:**

Description of incident:

Signed _____ Date _____

Result of enquiry/Action taken:

Signed _____ Date _____