

The Acorn School

ONLINE SAFETY POLICY

2018-2019

Written: January 2017

Reviewed and approved by Proprietors: September 2018

Graeme Whiting _____ *Sarah Whiting* _____

Approved by Headteachers: September 2018

James Whiting _____ *Barney Franklin* _____

Next review date: September 2019

ONLINE SAFETY RESPONSIBILITIES WITHIN THE ACORN SCHOOL

DESIGNATED ONLINE SAFETY LEAD:	James Whiting M: 07521 147690 E: jameswhiting@theacornschoo.com
PROPRIETORS	Graeme and Sarah Whiting T: 01453 832944 M: 07590646907 E: graemewhiting@theacornschoo.com
HEADMASTERS	James Whiting T: 07521147690 E: jameswhiting@theacornschoo.com Barney Franklin E: barneyfranklin@theacornschoo.com

Development, monitoring and review of this policy

This Online Safety policy has been developed by the proprietors and senior leadership team of the school and was approved in December 2016.

Monitoring of this online safety policy will take place at regular intervals and the proprietors will receive a report on the implementation of the policy, as laid out in the table below:

This Online Safety policy was approved by the Proprietors on:	January 11th 2018
The implementation of this Online Safety policy will be monitored by the:	Headmaster and Online Safety Lead
Monitoring will take place at regular intervals:	Once per term
The Proprietors will receive a report on the implementation of the Online Safety Policy generated by the Upper School Teachers (which will include anonymous details of online safety incidents) at regular intervals:	Once per term
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering

Scope of the Policy

This policy applies to all members of The Acorn School community (including staff, students, volunteers, parents / carers) who have access to and are users of the school's ICT systems, both in and out of The Acorn School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The Acorn 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 e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals within The Acorn School:

Proprietors

Proprietors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Proprietors receiving regular information about online safety incidents and monitoring reports. Proprietors of the school will:

- Have regular meetings with the Designated Online Safety Lead
- Attend Online Safety meetings
- Regularly monitor online safety incident logs
- Regularly monitor filtering / change control logs

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Designated Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will receive regular monitoring reports from the Designated Online Safety Lead.

Designated Online Safety Lead:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Liaises with school IT support provider
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, meets regularly with proprietors to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings
- Reports regularly to headmaster

The Online Safety Lead is also responsible for network management, which includes ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Group / other relevant body Online Safety Policy / Guidance that may apply.
- Those users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / Internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- They report any suspected misuse or problem to the Headteacher or Designated Online Safety Lead for investigation / action / sanction
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school emails. Text messaging students or parents/carers is not allowed.
- Online safety issues are embedded in all relevant aspects of the curriculum and other activities
- Students understand and follow the Online Safety Policy and acceptable use agreements
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies by students and uphold the school's ban on mobile devices in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Teachers must also support the school's ban on the use of any mobile phone within the school grounds. If a teacher needs to use their mobile phone under exceptional circumstances, they must only do so in the designated area of the school office.
- Staff are not permitted to follow or engage with students of the school on any personal social media network account.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data

- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students:

- Are responsible for using the school digital technology systems in accordance with the **Student Acceptable Use Agreement**
- Are to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Must support the school's ban on the use of any mobile phone within the school grounds or on school trips, except when asked to do so by a teacher.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the **school's Online Safety Policy** covers their actions out of school, if related to their membership of the school.
- Staff are not permitted to follow or engage with students of the school on any personal social media network account.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events. Parents must also support the school's ban on the use of any mobile phone within the school grounds, as a parent or a student.

Policy Statements

Education – Students

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

Online safety should be a focus in the curriculum and staff should reinforce it in an age-appropriate manner, taking into account the student's age and the Parents' Handbook and Charter. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of ICT and other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of tutorials and other learning activities
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Students below class 11 (17 years old) are not allowed to use the internet in school time, at all. Where class 11 and 12 students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- **Computers or laptops are forbidden from being used outside of lessons where they are explicitly told they may be used. Under no circumstances may computers or laptops be used in lessons where students below class 11 are present (except where allowed by teacher), or during break times, lunchtimes, before school.**
- It is accepted that from time-to-time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Designated Online Safety Lead can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be recorded, with clear reasons for the need.

Education – Parents / Carers

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

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

- Letters
- Parents' evenings
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk) www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL / 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 teachers' meetings.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password to access school IT equipment. Users are responsible for the security of their username and password.
- The school has provided high-level filtering through the SWGFL.
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- No ITC equipment is allowed to be used by students out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the online safety lead.
- Users may use the following types of removable media for the purposes detailed:

- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Use of teachers’ and students’ own devices

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, 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 and other services such as email and data storage.

All users should understand that the primary purpose of the use of personal devices in a school context is educational. The use of technologies policy should be in agreement with other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme.

The school allows students and teachers to use personal laptops in school, with prior permission, but telephones, tablets, Kindles, gaming devices and other electronic devices are not allowed. Teachers are allowed to use mobile phones in the office only, and only in exceptional circumstances.

Use of digital and video images

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

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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 students in the digital / video images.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images, which include students or members of staff, should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Staff must ensure that they:

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

- The data must be encrypted and password protected. See James for advice and instructions on this.
- The device must be password protected
- The device must offer approved virus and malware checking software. The office will provide a list of approved software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for young people to understand what is expected of their behaviour and attitude when using the Internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School should encourage parents/carers to support the agreement with their young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any student found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions, which could include not being allowed to access the Internet for a period of time.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

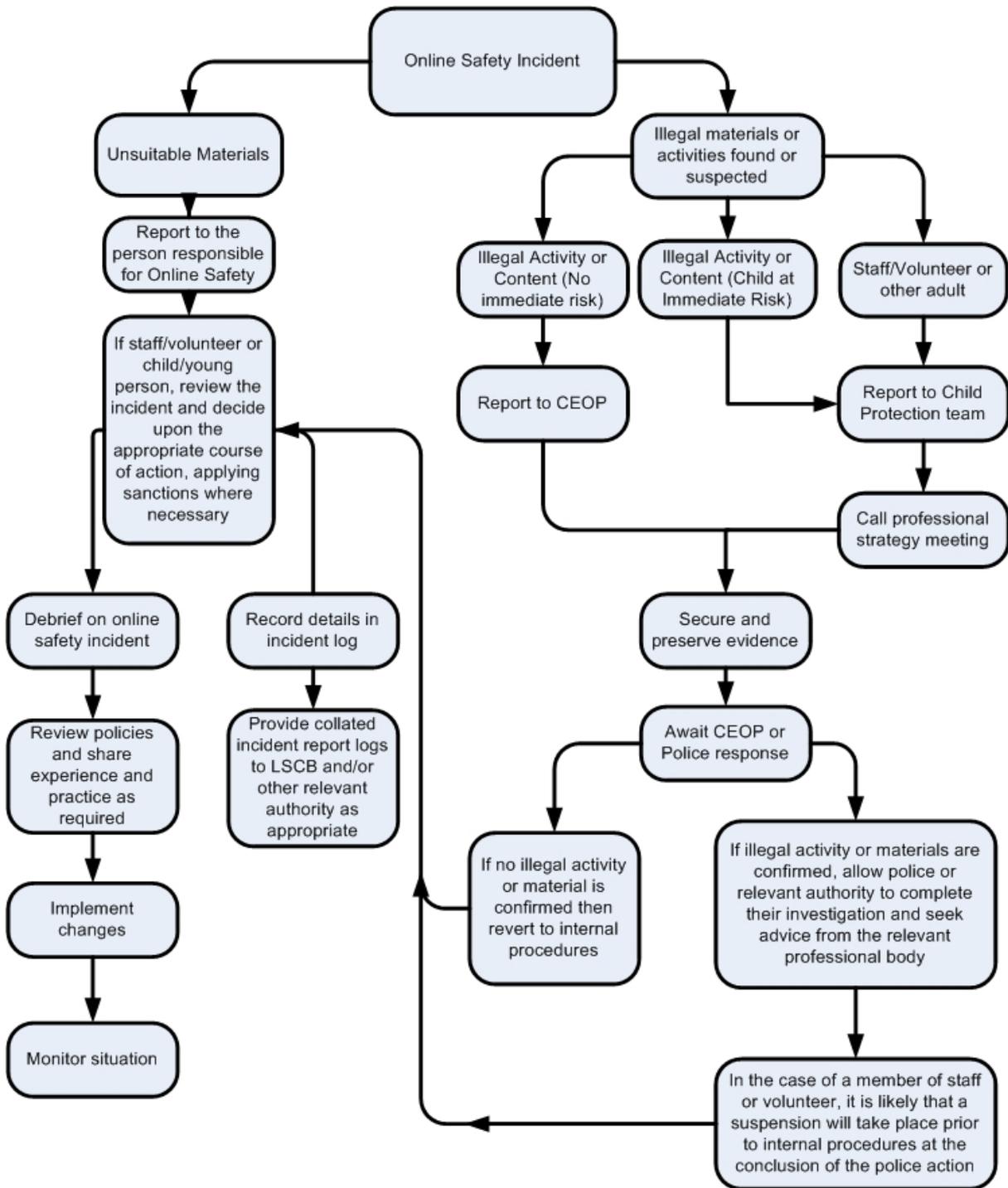
Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staff 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 involve illegal or inappropriate activities (see “In the Event of Inappropriate Use” above). See flow chart on the next page.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and [follow the](#) school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the 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 Group 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
 - Adult material which potentially breaches the Obscene Publications Act
 - Criminally racist material
 - Promotion of terrorism or extremism
 - Other criminal conduct, activity or materials
 - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

Any misuse of the school’s ICT systems, by staff or students, should be reported to the headmaster immediately. If the incident includes activities considered illegal, the police and other relevant bodies will be involved immediately, by the headmaster.

The Acorn School

ACCEPTABLE USE AGREEMENT

STUDENTS

2017-2018

School Policy

Despite the strong stance on the use of electronics and the Internet in young children, The Acorn School understands the importance and benefits that arise from the safe and appropriate use of ICT equipment, including the Internet. New technologies have become integral to the lives of young people, both within school and outside school, and the school aims to ensure that young people are safe when using the Internet, at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse.
- That students have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Your activity on the Internet is closely monitored by the school; logs are kept of activity, whether on a school device or using your own device through the school network. These logs include who is accessing what material for how long from which device.

Acceptable Use Policy Agreement

I understand that I must use The Acorn School's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

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

- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that the school has given me the right to use digital technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use.
- I will not use the school systems or devices, or my personal device in school, for on-line gaming, on-line gambling, Internet shopping, file sharing, **social media** or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

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

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

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve

my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school Internet, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

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

Student Acceptable Use Agreement Form

2017-2018

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

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

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. laptops, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school (e.g. communicating with other members of the school).

Name of Student / Pupil:

Class:

Signed:

Date:

The Acorn School Office Use Only

Received by The Acorn School:

Name: _____ **Date:** _____

Signature: _____

The Acorn School

ACCEPTABLE USE AGREEMENT

STAFF

2017-2018

School Policy

Despite the strong stance on the use of electronics and the Internet in young children, The Acorn School understands the importance and benefits that arise from the safe and appropriate use of ICT equipment, including the Internet. New technologies have become integral to the lives of young people, both within schools and outside school, and the school aims to ensure that young people are safe when using the Internet, at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students 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, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work.

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) 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.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites in school.
- I will only communicate with students and parents / carers using official school email. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using 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 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.
- I will not try to upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, or referral to the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the school's Online-Safety Policy and Acceptable use Agreement 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: