The Attic
Online Safety Policy

Date of policy	June 2017
Date presented to Management Committee	July 2017
Date ratified by Management Committee	July 2017
Date for review	July 2018

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Additional note:
The Attic Pupil Referral Unit wishes it to be known that it takes very seriously the naming of professional staff in social media forums, such as Facebook and Twitter, and, in particular any comments that are deemed negative and can have an impact of the well-being of school staff. The school reserves the right to take action against claims or commentary if a member of staff feels their professional integrity is being called into question.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Managers:
Managers 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 *Managers* receiving regular information about Online Safety incidents and monitoring reports. A member of the Management Committee has taken on the role of *Online Safety Manager*. The role of the Online Safety Manager will include:
• *regular meetings with the Online Safety Lead*
• *regular monitoring of Online Safety incident logs*
• *regular monitoring of filtering / change control logs*
• *reporting to relevant Managers meeting*

Head teacher and Senior Leadership Team :
• **The Head teacher is responsible 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 *Online Safety Lead*.
• *The Head teacher/Senior Leadership Team are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.*
• *The Head teacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
• *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*
• **The Head teacher and 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.** (See the flow chart on dealing with Online Safety incidents taken from the Suffolk

County Council Hub – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures).

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

- liaises with JCComtech.

• receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
• meets regularly with Online Safety Manager to discuss current issues, review incident logs and filtering/ change control logs.
• attends relevant Managers meetings.
• reports regularly to Senior Leadership Team.
• co-operates with Head teacher and/or Senior Leadership Team regarding investigation of any incidents that require further actions, or disciplinary sanctions.

JCComtech:

JCComtech in consultation with the administrative assistant is responsible for ensuring:

• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
• that the school meets the Online Safety technical requirements outlined by the Local Education Authority Security Policy, the Acceptable Use Policy and any relevant guidance.
• that users may only access the school's networks through an enforced password protection policy.
• that E2BN is informed of issues relating to the filtering applied by the Suffolk School's Private network.
• *that the school's filtering policy, is applied and updated on a regular basis on the advice of the Online Safety working party.*
• that he/she keeps 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/Virtual Learning Environment ()/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Online Safety Lead /Head teacher/Senior Leadership Team for investigation/action/sanction.*
• *that monitoring software/systems are implemented and updated as agreed in school policies.*

Teaching and Support Staff

are responsible for ensuring that:

• they have an up to date awareness of Online Safety matters and of the current school E- safety policy and practices.
• they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
• they report any suspected misuse or problem to the Online Safety Lead/ Head teacher/ Senior Leadership Team for investigation/action/sanction.
• digital communications with pupils (e.g. using the Virtual Learning Environment ()) should be on a professional level *and only carried out using official school systems.*
• Online Safety issues are embedded in all aspects of the curriculum and other school activities.
• pupils understand and follow the school Online Safety and acceptable use policy.
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• they monitor ICT activity in lessons and extra curricular school activities.
• they are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
• *in lessons where internet use is pre-planned pupils 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.*

Designated Safeguarding Lead or Alternate Designated safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protection 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
• is aware that Online Safety issues are child protection issues and not just technical issues, simply that the technology provides additional means for the child protection issues to develop.

Pupils:
• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
• will be taught to have an appropriate 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school. They should understand that the school will respond to any actions committed outside of school using digital technologies where the action is having an impact within school.
• understand the need to deposit mobile phones at the school office during school hours for collection at the end of the day, and appreciate that the school has the right to view (and where necessary delete) any photos taken in school.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues

Parents and carers will be responsible for:
• endorsing (by signature) the Pupil Acceptable Use Policy.
• accessing the school website in accordance with the relevant school Acceptable Use Policy.

Important Additional Note
The Attic Pupil Referral Unit wishes it to be known that it takes very seriously the naming of professional staff in social media forums, such as Facebook and Twitter, and, in particular any comments that are deemed negative and can have an impact of the well-being of school staff. The school reserves the right to take action against claims or commentary if a member of staff feels their professional integrity is being called into question.

Community Users
Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.
Important Additional Note
The Attic Pupil Referral Unit wishes it to be known that it takes very seriously the naming of professional staff in social media forums, such as Facebook and Twitter, and, in particular any comments that are deemed negative and can have an impact of the well-being of school staff. The school reserves the right to take action against claims or commentary if a member of staff feels their professional integrity is being called into question.

Policy Statements

Education – pupils

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 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 education will be provided in the following ways:

• A planned Online Safety programme should be provided as part of both ICT and PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

• Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

• Pupils 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.

• Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

• Pupils will be taught Digital Citizenship, i.e. how to be a good citizen online.

• Guidance on the use of ICT systems / internet will be displayed.

• Staff should act as good role models in their use of ICT, the internet and mobile devices.

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

• Newsletters, web site,

Education & Training – Staff

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. An audit of the Online Safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify Online Safety as a training need within the performance management process.*

• 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 Policies.
• The Online Safety Lead and/or JCComtech will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released.
• This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET.
• The Online Safety Lead will provide advice / guidance / training as required to individuals as required.
Training – Managers
Managers should take part in Online Safety training / awareness sessions, with particular importance for those who are involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways:
• Attendance at training provided by the Local Authority or other relevant organisation.
• Participation in school training / information sessions for staff or parents.
Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:
• School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in any relevant Local Authority Online Safety Policy and guidance.
• There will be regular reviews and audits of the safety and security of school ICT systems.
• Servers, wireless systems and cabling must be securely located and physical access restricted
• All users will have clearly defined access rights to school ICT systems. *Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the Online Safety Working Party.*
• All users will be provided with a username and password by *JCComtech who will keep an up to date record of users and their usernames. Users will be required to change their password approximately every term.*
• The "master / administrator" passwords for the school ICT system, used by the JCComtech and Administrative Assistant must also be available to the Head teacher and kept in a secure place (e.g. school safe).
• Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
• The school maintains and supports the managed filtering service provided by E2BN, in accordance with the Web Control Filtering Policy.
• In the event of the JCComtech and Administrative Assistant *needing to switch off the filtering for any reason, or for any user, this must be logged.*
• Any filtering issues should be reported immediately to JCComtech.
• JCComtech regularly monitors and records the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
• Remote management tools are used by the JCComtech to control workstations and view user's activity.

• A reporting system is in place for users to report any actual / potential Online Safety incident.
• 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.
• An agreed procedure is in place to provide temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
• The filtering policy deals adequately with the downloading of executable files by users.
• The acceptable use policy limits the scope of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
• The schools accepted procedure is to block the installation of programmes onto school workstations / portable devices.
• The acceptable use policy describes the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
• The school infrastructure and individual workstations are protected by up to date virus software.
• Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. School reports should be sent to the head teacher using the school based email system.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

• in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
• Where 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.
• It is accepted that from time to time, for good educational reasons, pupils 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 JCComtech (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
• Pupils 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.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate 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.

*• 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. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.*
• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Pupils must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year* see Parents / Carers AUP Agreement in the appendix).
• *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• 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.

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

• the data must be encrypted and password protected.
• the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
• the device must offer approved virus and malware checking software.
• the data must be securely deleted from the device, in line with school policy, once it has been transferred or its use is complete.

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

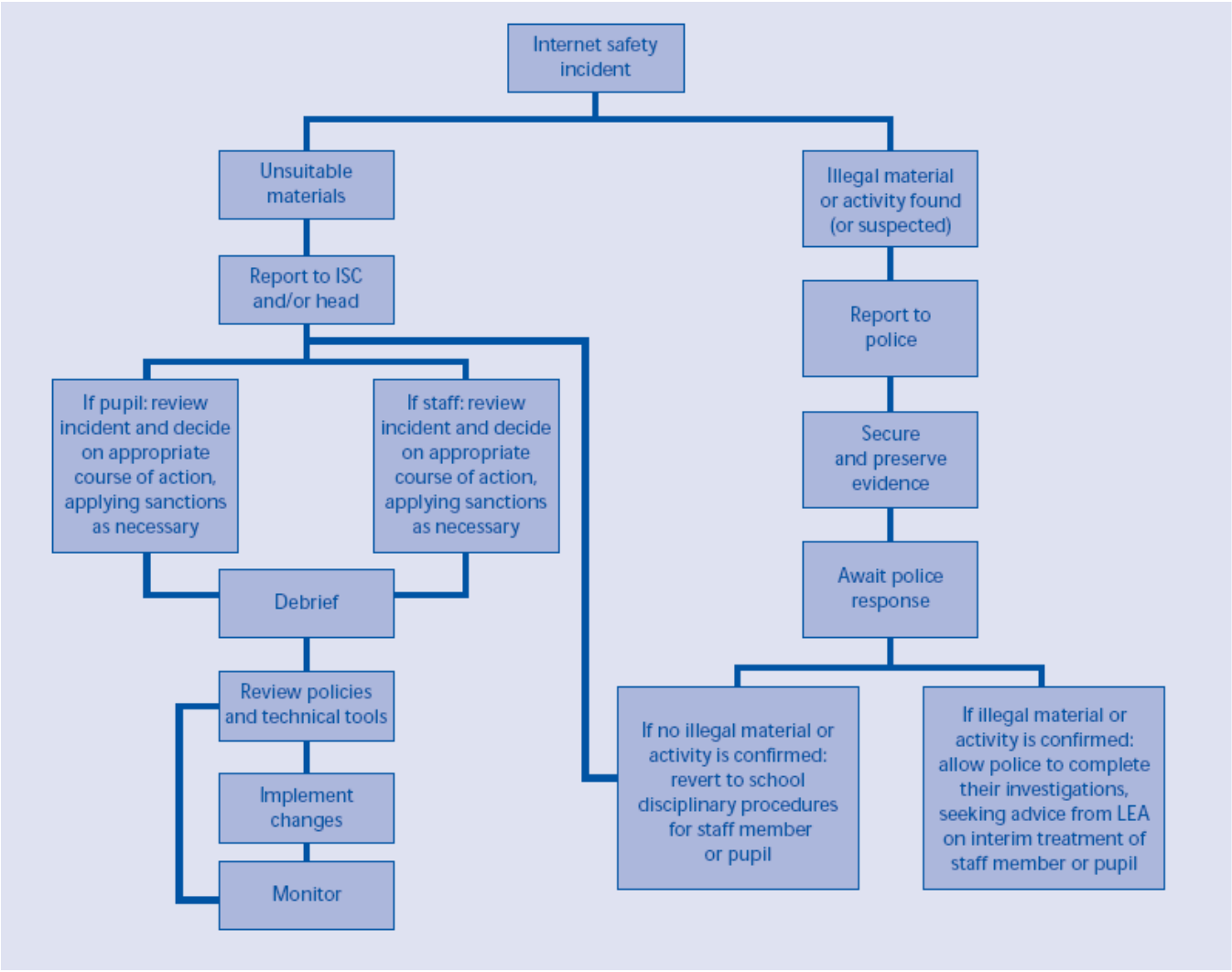
• The official school email service may be regarded as safe and secure and is monitored. *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
• Users need to be aware that email communications may be monitored
• Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
• Any digital communication between staff and pupils or parents / carers (email, etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*

• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Responding to incidents of misuse
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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity i.e.
- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The flow chart below from the Suffolk CC Hub / ICT / Online Safety should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer (e.g. the Head Teacher Laptop).
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:



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer (e.g. the Head Teacher Laptop).

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.