Archbishop Temple School

A Church of England Specialist College

ONLINE SAFETY POLICY

Date Agreed : March 2021

To Be Reviewed : March 2023

Name of Policy: **Online Safety Policy**

Sub-Committee Responsible: **Governors’ Pastoral, Community & Chaplaincy (PCC) Committee**

Lead Responsibility in School: **Assistant Headteacher DEARR & IT Network and Firefly**

Source of Policy: (Please tick)

- ○ **LA:**
- ○ **Diocesan:**
- ○ **School: X**
- ○ **Other – Please specify:**

This policy supports our work as a Church school as summarised in our Vision Statement:

Purpose
Archbishop Temple School seeks to care for young people and prepare them well for adulthood, valuing the whole person.

Mission
Through our faith in God, Father, Son and Holy Spirit, we strive to nurture each person’s ability, gifts and talents so that they can ‘have life and have it to the full’ (John 10:10) and use it in the service of God and other people.

Purpose of the Policy	The aim of this policy is to provide guidance to all members of the Archbishop Temple School community about e safety
Staff responsible for the policy	• Headteacher • Assistant Headteacher DEARR (IT systems) • Assistant Headteacher SENCo (iPads) • Assistant Headteacher Director of Pupils • Online Safety Coordinator • IT Network Manager
Related Material	• ATS Behaviour Policy • Safeguarding Policy • RSE Policy • Staff Code of Conduct • ATS Staff Disciplinary Codes • ATS Data Protection Policy • ATS Confidentiality Policy • iPads for Learning Agreement • Live Lesson Acceptable Use Policy (Part of Staff and volunteer ICT Acceptable Use Policy) • Staff and volunteer ICT Acceptable Use Policy • Pupil ICT Acceptable Use Policy • Online Learning Policy • Keeping Children Safe in Education September 2020 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892394/Keeping_children_safe_in_education_2020.pdf • Teachers' Professional Standards - https://www.gov.uk/government/publications/teachers-standards • SWGFL Model Policy - https://swgfl.org.uk/resources/online-safety-policy-templates/#downloads
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.	

Scope of the Policy

This policy applies to all members of the Archbishop Temple School community (including staff, students, volunteers, parents/carers, visitors) who have access to and are users of school's ICT systems, both in and out of the school.
Incidents of cyber-bullying or other online safety incidents are covered by this policy, which may take place outside of the school but are 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.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current school online safety policy and practices. Staff are provided with continuous CPD to keep them updated of the latest online safety developments;
- they have read, understood and signed the Staff and volunteer ICT Acceptable Use Policy including the Live Lesson Acceptable Use Policy;
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation and then this is passed on to the relevant Assistant Headteacher (for misuse of iPads – AHT SENCo and for all other misuse – AHT DEARR) for action/sanction;
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities. Departments are responsible for ensuring that online safety is written in to schemes of work, where appropriate, and department handbooks;
- students understand and follow the Online Safety and Acceptable Use policies;
- 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, mobile devices, cameras etc. in lessons and other school activities (where allowed) 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 through internet searches.

Designated Senior Leaders for safeguarding 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 Policy, iPads for Learning Agreement and Online Learning Policy;
- 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 mobile devices and digital cameras. They should also know and understand 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.

Parents/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 are not allowed to be shared on social media websites;
- access to parents' sections of the website/VLE;
- their children's iPad for Leaning;
- social media accounts minimum age guidance;
- take responsibility for their child's online safety at home.

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 all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- a planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited;
- key online safety messages should be reinforced as part of a planned programme of assemblies, Morning Reports in tutorial time and PSHE activities;
- students should be taught to be critically aware of the materials/content they access online 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 helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- where students are allowed to freely search the internet, 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, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated 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.

Education – Parents/Carers

Archbishop Temple School will seek to provide information and awareness to parents and carers through:

- curriculum activities;
- website and Firefly;
- parent/carers evenings;
- high profile events/campaigns e.g. Safer Internet Day

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 is delivered to staff in morning briefings, inset days and meetings. 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's Online Safety Policy and Acceptable Use Agreements;
- the Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- this Online Safety Policy and its updates will be presented to and discussed by staff;
- the Online Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors

Governors take part in online training/awareness sessions. This is offered in a number of ways:

- attendance at training provided by the Local Authority/National Governors Association or other relevant organisation;
- participation in school training/information sessions for staff or parents;
- online training;
- at PCC meetings.

Technical – infrastructure/equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school is also responsible for ensuring that the relevant people named in the above sections are 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 the school's technical systems by Virtue;
- servers, wireless systems and cabling must be securely located and physical access restricted;
- all users will have clearly defined access rights to the school's technical systems and devices;
- all users will be provided with a username and secure password by the IT network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and that it is set to a minimum requirement of 8 characters including upper and lowercase, a number and prefix;
- all users will be asked to change their password every six months - 1st week in December and 1st week in June.
- The "administrator" passwords for the school ICT system, used by the IT network manager must also be available to the Headteacher and Assistant Headteacher – DEARR, IT network & Firefly and kept in a secure place;
- The IT network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband filtering provider (Virtue). **Content lists are regularly updated** and internet use is logged and regularly monitored. (There is a clear process in place to deal with requests for filtering changes);
- Through the IT network manager, the school has provided enhanced user-level filtering (allowing different filtering levels for different groups of users – staff/students etc);
- The IT network manager regularly monitors and records the activity of users on the school technical 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 technical incident/ security breach to the relevant person, as agreed);

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software (Sophos);
- an agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems;
- an agreed policy is in place regarding the extent of personal use that users (staff/students) and their family members are allowed on school devices that may be used out of school;
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices;
- an agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured;
- from September 2017 no pupils will be allowed to use removable media in school (eg memory sticks/CDs/DVDs);
- staff are requested to submit school devices for audit purposes twice a year to ensure correct usage in line with the online safety policy.

iPads for Learning

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. In order to support the learning of all pupils in school, since May 2015 the school has introduced iPads for Learning and applies to all school years. An overwhelming majority of parents supported the school's vision and have either contributed to the monthly payment scheme, bought an iPad outright or opted for their child to BYOD. The small minority of pupils who have not taken part in the programme are provided an iPad to use during the school day. All students and parents have signed an iPads for Learning Agreement which clearly sets out the framework of use. All iPads used in school are required to be registered with the schools MDM (Lightspeed) this system is aimed at reducing potential vulnerabilities into existing secure environments.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the GDPR principles as outlined in the GDPR policy.
- All users are provided with and accept the Acceptable Use Agreements.
- All network systems are secure and access for users is differentiated.
- All iPad for learning devices will be registered to the school's MDM and covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Mandatory training is undertaken by all staff.
- Students receive training and guidance on the use of personal devices in lessons and Year group assemblies.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported to our IT Network Manager.
- Any user leaving the school will follow the process outlined within the iPad for Learning Agreement.

Cyber bullying/youth produced sexual imagery
Use of mobile devices
Mobile phones, tablets, games consoles, digital cameras, voice recording devices, etc.

We currently do not allow any mobile devices other than iPads for Learning devices to be used in school under any circumstances without the express permission from a teacher. All phones should be stored securely in jackets, bags or lockers whilst on school premises and switched off.

The following statements must be considered when using these devices:

- That some mobile devices e.g. mobile phones, game consoles or tablets can access unfiltered internet content.
- That any devices used outside of school are virus checked before use on school systems.

In our school the following statements outline what we consider to be acceptable and unacceptable use of mobile telephones:

- Mobile phones are not permitted in school for children's use, unless expressed permission is given by a teacher. Staff should ensure their own phones are turned off/silent and not used in the classroom or any communal space in view of pupils.
- It is acceptable to use personal mobile phones for school activities e.g. school trips. However, under no circumstances should staff be giving pupils their personal mobile phone numbers.
- A school mobile phone is made available for activities where a personal mobile phone maybe considered inappropriate, e.g. school trips, after-school events.
- ParentApp is used to give notification to parents of club times and messages. These are only sent by the Headteacher, Headteacher's PA, Marketing and PR Officer, Pastoral Manager, Exams Officer, Receptionist and School Business Support Officer.
- Staff are not allowed to use personal mobile phones or other personal devices to take pictures of pupils whilst in school, taking part in activities or on trips. Staff should only use school iPad devices or the school cameras when taking pictures.

Use of Firefly

Our VLE, Firefly, offers the school a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It enables pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- Pupils/staff will be advised about acceptable conduct and use when using Firefly.
- Only members of the current pupil, parent/carers and staff community will have access to Firefly.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, pupils etc leave the school their account or rights to specific areas will be disabled.

Radicalisation and Extremism

The school's Child Protection Policy which is available on our website http://www.archbishoptemple.com/policies-and-procedures/11072.html and in school, covers Radicalisation and Extremism.

Indicators of vulnerability to extremism and radicalisation

- Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- Extremism is defined by the Government in the Prevent Strategy as: Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

- Extremism is defined by the Crown Prosecution Service as *The demonstration of unacceptable behaviour by using any means or medium to express views which:*
  - encourage, justify or glorify terrorist violence in furtherance of particular beliefs;
  - seek to provoke others to terrorist acts;
  - encourage other serious criminal activity or seek to provoke others to serious criminal acts;
  - foster hatred which might lead to inter-community violence in the UK;
  - there is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity;
  - pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

Indicators of vulnerability include

- Identity Crisis – the student/pupil is distanced from their cultural/religious heritage and experiences discomfort about their place in society.
- Personal Crisis – the student/pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
- Personal Circumstances – migration; local community tensions; and events affecting the student/ pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
- Unmet Aspirations – the student/pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
- Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement/reintegration.
- Special Educational Need – students/pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.
More critical risk factors could include:

- being in contact with extremist recruiters;
- accessing violent extremist websites, especially those with a social networking element;
- possessing or accessing violent extremist literature;
- using extremist narratives and a global ideology to explain personal disadvantage;
- justifying the use of violence to solve societal issues;
- joining or seeking to join extremist organisations;
- significant changes to appearance and/or behaviour;
- experiencing a high level of social isolation resulting in issues of identity crisis and/or personal crisis.

Preventing violent extremism

The Assistant Headteacher Director of Pupils is the school’s safeguarding lead and is responsible for:

- ensuring that staff of the school are aware of the Safeguarding Lead’s role in relation to protecting students/pupils from radicalisation and involvement in terrorism;
- maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism;
- raising awareness about the role and responsibilities of Archbishop Temple School in relation to protecting students/pupils from radicalisation and involvement in terrorism;
- monitoring the effect in practice of the school’s RE curriculum to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism;
- acting as the first point of contact within the school for case discussions relating to students/ pupils who may be at risk of radicalisation or involved in terrorism.

Use of digital and video images

- 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.
- 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 in not covered by the GDPR). 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 and volunteers 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. All images of school events should be placed in the staff shared area and not in their own personal areas or on the pupil shared area. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Images should be removed from staff devices and placed on the secured staff shared area immediately.
- 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 including other school social media accounts 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.
- Written permission from parents/carers will be obtained before photographs of students are published on the school website.
- Student’s work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) 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.

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- every effort is made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing";
- it has a Data Protection Policy;
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- risk assessments are carried out;
- it has clear and understood arrangements for the security, storage and transfer of personal data. This means that any devices that are taken off site are encrypted by the IT network manager;
- data subjects have rights of access and there are clear procedures for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data. This is undertaken by the IT network manager. Past pupil information is to be deleted from Firefly and the servers as of November of their year of graduation;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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, memory stick or any other removable media:

- the data must be encrypted and password protected;
- the device must 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 (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 and can be accessed by the Headteacher at any time.
- 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/students or parents/carers should be through email or Firefly only and 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

The school has a duty of care to provide a safe learning environment for students and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- training to include acceptable use, social media risks, checking of settings, data protection, reporting issues;
- clear reporting guidance, including responsibilities, procedures and sanctions (see behavior policy)
- Risk assessment, including legal risk.

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;
- 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 by the the IT network manager to ensure compliance.

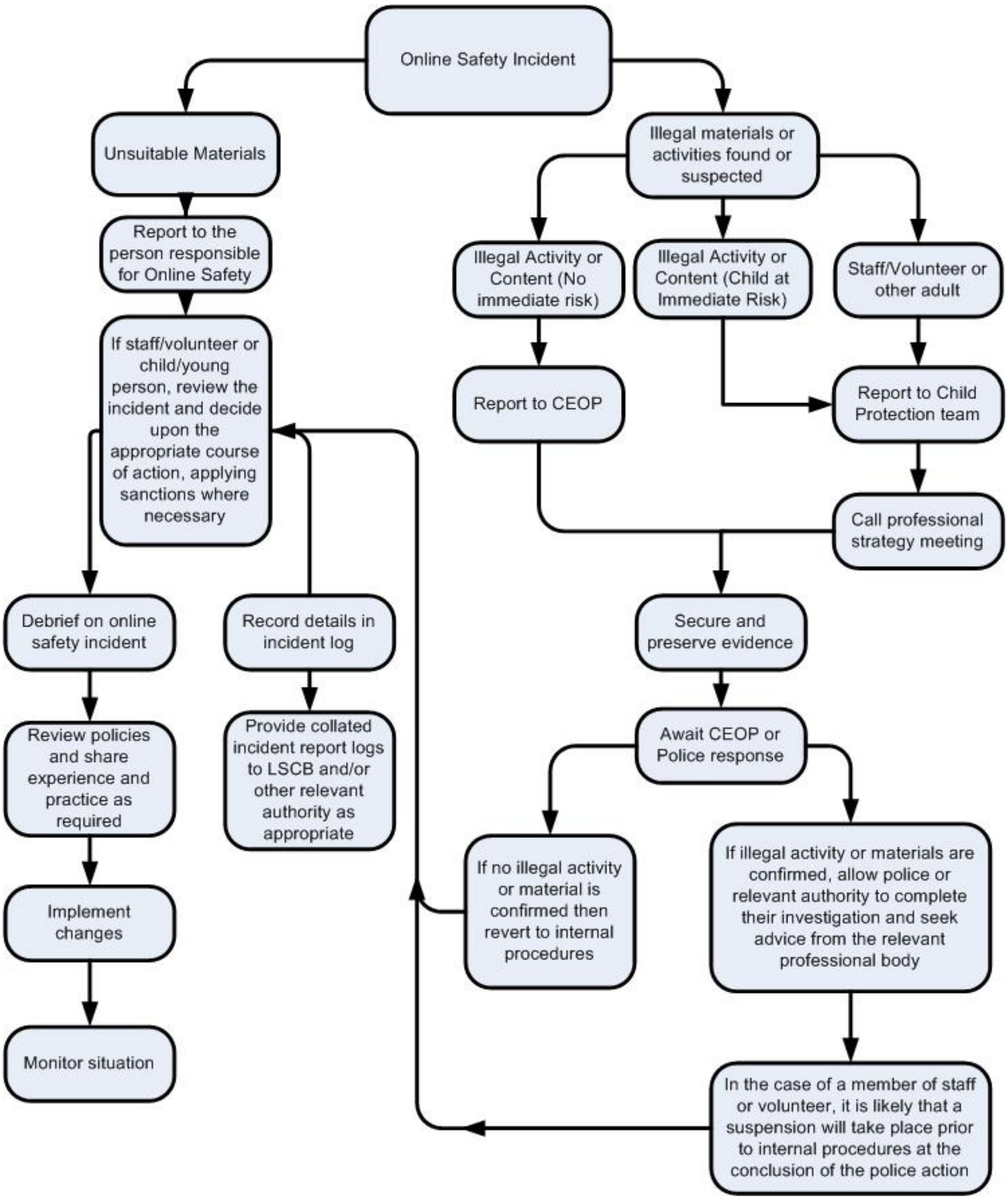
Unsuitable/inappropriate activities

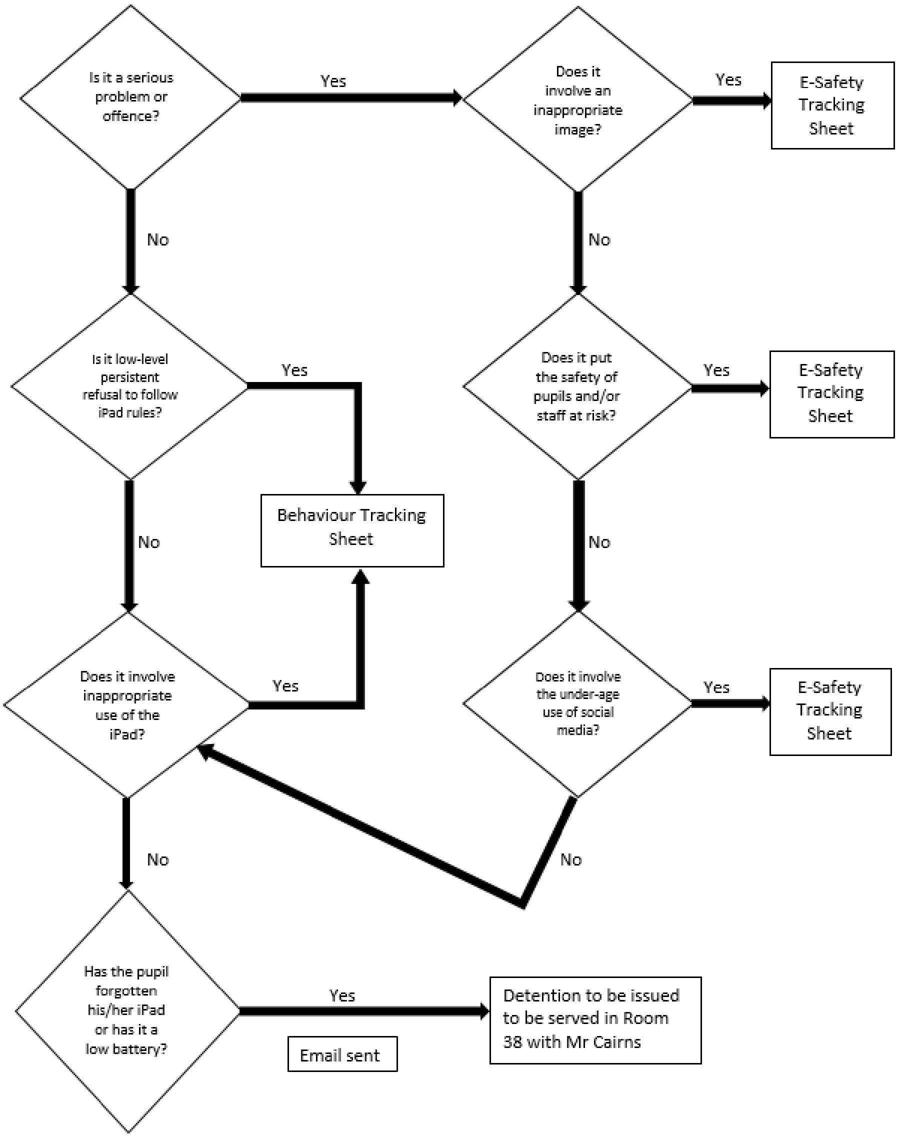
The school believes that the activities referred to below would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The following list is not exhaustive. Users should be aware that the school’s disciplinary and behaviour codes will be used in dealing with any infringements.

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:

- child sexual abuse images – the making, production or distribution of indecent images of children contrary to The Protection of Children Act 1978;
- grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003;
- possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008;
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986;
- pornography;
- promotion of any kind of discrimination threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- using school systems to run a private business;
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- infringing copyright;
- 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;
- unfair usage (downloading/uploading large files that hinders others in their use of the internet);

Responding to incidents of misuse


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action


Is it a serious problem or offence?
Yes
No
Does it involve an inappropriate image?
Yes
E-Safety Tracking Sheet
No
Is it low-level persistent refusal to follow iPad rules?
Yes
Behaviour Tracking Sheet
No
Does it put the safety of pupils and/or staff at risk?
Yes
E-Safety Tracking Sheet
No
Does it involve inappropriate use of the iPad?
Yes
No
Does it involve the under-age use of social media?
Yes
E-Safety Tracking Sheet
No
Has the pupil forgotten his/her iPad or has it a low battery?
Yes
Detention to be issued to be served in Room 38 with Mr Cairns
Email sent

Illegal Incidents

If there is any suspicion that the website(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 for responding to online safety incidents and report immediately to the police. All complaints about internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the Headteacher.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow 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 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 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;
  - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

In dealing 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.

Monitoring

The school will monitor the impact of the policy using:

- logs of reported incidents;
- monitoring logs of internet activity (including sites visited);
- internal monitoring data for network activity;
- surveys/questionnaires of:
  - students
  - parents/carers
  - staff.

The Online Safety Committee will receive a report on the implementation of the Online Safety Policy generated by the E-safety Coordinator at regular intervals.