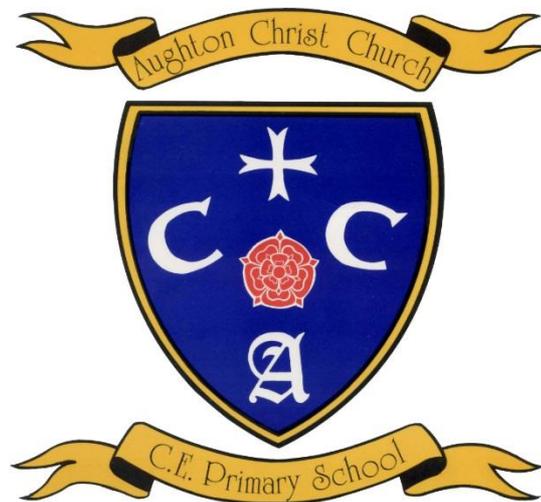


Policy Document

Aughton Christ Church C of E Primary School

Online Safety Policy



Reviewed: Spring 2019
Next Review date: Spring 2020

Aughton Christ Church C E Primary School



Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling incidents
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Social networking

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Introduction and Overview Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Aughton Christ Church C of E Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation. etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image) □

Sexting

- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Aughton Christ Church C of E Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Aughton Christ Church C of E Primary School IT systems, both in and out of Aughton Christ Church C of E Primary School

Roles and responsibilities

Role	Key Responsibilities
Designated Child Protection Lead	<ul style="list-style-type: none">• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents• Promote an awareness and commitment to online safety throughout the school community• Ensure that online safety education is embedded within the curriculum• Liaise with school technical staff where appropriate• To communicate regularly with SLT and the governors to discuss current issues, review incident logs and filtering/change control logs• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident• To ensure that online safety incidents are logged.• Facilitate training and advice for all staff• Liaise with the Lancashire County Council and relevant agencies (APEX and Dr. R Musker)• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Designated Senior Lead	To ensure that the school has in place policies and practices to keep the children and staff safe online

Role	Key Responsibilities
	<ul style="list-style-type: none"> • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Curriculum Leader	<ul style="list-style-type: none"> □ To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician (APEX)	<ul style="list-style-type: none"> • To report online safety related issues that come to their attention, to the DSL • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. <ul style="list-style-type: none"> - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Teachers	<ul style="list-style-type: none"> • To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
All staff, volunteers and contractors.	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. New staff on induction sign the AUP. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology <p>Exit strategy</p> <ul style="list-style-type: none"> • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	<ul style="list-style-type: none"> • To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/children • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images

Role	Key Responsibilities
External groups including Parent groups	<ul style="list-style-type: none"> • Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Senior Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Designated Senior Lead that day.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies.

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Education and Curriculum

Pupil Online Safety

Curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience.
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s)
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents which includes online safety
- runs a rolling programme of online safety advice, guidance and training for parents.

Expected Conduct and Incident management

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good online safety practice when using digital technologies in and out of school
- know and understand school policies on the use of mobile and hand held devices including cameras

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

This school

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- support is sought from other agencies as needed in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school

- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities.

Managing IT and Communication System

Internet Access, security (Virus Protection) and Filtering

This school:

- informs all users that Internet/email use is monitored
- has the educational filtered secure broadband connectivity through the LGfL
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- uses USO user-level filtering where relevant
- ensures network health through use of Sophos anti-virus software (from LGfL)
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protectlevel' (sensitive personal) data off-site
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Has additional local network monitoring/auditing software installed
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies
- Has daily back-up of school data (curriculum)
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#)

- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU. To ensure the network is used safely, this school:
- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password
- All pupils have their own unique username and password which gives them access to the Internet and other services
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to log off when they have finished working or are leaving the computer unattended
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others, If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to change their passwords into the LGfL email, when prompted by the authority.

E-mail

This school:

- Provides staff with an email account for their professional use, Lancashire LA Staff email and makes clear personal email should be through a separate account
- We use anonymous or group e-mail addresses, for example bursar@schoolname.lancs.sch.uk/head@schoolname.lancs.sch.uk/or class e-mail addresses.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required which will be reviewed annually.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
-

Data security: Management Information System access and Data transfer.

Strategic and Operational Practices

This school:

- The Head Teacher is the Designated Senior Lead).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- Mobile devices are not permitted to be used in certain areas within the school site, staff room and offices.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored in the school office. They must remain turned off and out of sight until the end of the day.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times in designated areas, out of view from children.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by APEX.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital Images and Video

This school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school and change keystage.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Policy reviewed Spring 2019
Policy to be reviewed Spring 2020