Great Arley School

Our vision

- To become a great provider and recognised leader of SEND in Lancashire
- To provide the right curriculum that is personalised for every child to ensure they reach their full potential
- To provide a safe & thriving environment for both staff and pupils where wellbeing is paramount

Dare to Dream, Aim to Achieve

ONLINE SAFETY, CYBER SECURITY & ACCEPTABLE USE POLICY (For all stakeholders)

DATE REVIEWED	REVIEWED BY	NEXT REVIEW DATE
Autumn 2026	Nicola Holland	Autumn 2027

Great Arley School, Holly Road, Thornton, Lancashire, FY5 4HH
TELEPHONE – 01253 821072
WEBSITE – www.greatarley.lancs.sch.u

Online Safety – A School Policy and Charter for Action

INTRODUCTION:

This policy applies to all members of the school community (including staff, pupils, parents/carers, governors, volunteers, visitors and school community users) and should be read in conjunction with the Safeguarding and Child Protection policy, the school Behaviour Policy and the Artificial Intelligence policy.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety and Acceptable Use policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety and Acceptable Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

Our Commitment to Online Safety:

At Great Arley we discuss, monitor and review our Online Safety and Acceptable Use policy and procedures annually. We also subscribe to 360 degree safe audit tool Online Safety Self-Review Tool for Schools | 360safe. Our IT provider (Comptech) have also conducted a cyber security audit.

We support staff in the use of IT as an essential tool for teaching and learning and in the embedding of online safety across the whole school curriculum.

We also ensure, through our Computing and PSHE curriculums, that pupils understand the potential risks associated with the use of IT, mobile and internet technologies; that all online safety concerns will be dealt with sensitively and effectively; that pupils feel able to and safe to report incidents or worries and concerns they have and that they abide by our school's Online Safety and Acceptable Use Policy, including the Acceptable Use Agreement for pupils, when using IT and the internet. (Appendix 1). Other agreements listed in Appendix 1 include the Acceptable Use of the Internet: Agreement for Parents and Carers and Acceptable Use of the School's ICT Facilities and the Internet: Agreement for Staff, Governors, Volunteers and Visitors

We provide opportunities for parents and carers to receive online safety education and information to enable them to support their children in developing good online safety behaviour, whilst keeping them safe on-line. The school will report back to parents and

carers any online safety concerns. We encourage parents and carers to work with the school to uphold this policy and report any concerns they have.

We seek to learn from online safety good practice elsewhere and utilise the support of the Local Authority (LA) and relevant organisations when appropriate.

Purpose of the Online Safety and Acceptable Use Policy:

An effective whole school Online Safety and Acceptable Use policy is one which provides clear direction to staff, pupils, parents, governors and others about expected codes of behaviour in dealing with online safety issues. An effective policy also makes explicit the school's commitment to the development of good practice and sound procedures.

For the purposes of this policy the term child will include all pupils aged 4-16.

At Great Arley we are working with our staff, pupils and parents and carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of IT and follows agreed policies to minimise potential online safety risks.

Our Online Safety Champion:

The online safety champion in school is Nicola Holland, school DSL. She will be supported in this role by Oonagh Kearney, Jenny Keogh and Katrina Callaghan who are deputy DSLs.

The roles of these staff, including the Online Safety Champion are:

To be responsible for ensuring the development, maintenance and review of the Online Safety and Acceptable Use policy together with associated policies and documents.

To ensure that the policy is implemented and that compliance with the policy is actively monitored.

To ensure all staff are aware of reporting procedures and requirements should an online safety incident occur and that this must be reported to the Online Safety Champion who will then inform the Headteacher.

To ensure that all incidents are recorded on CPOMS and filtering and monitoring logs if required.

To keep up-to-date with online safety issues, guidance from the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection

Centre (CEOP) and www.saferinternet.org and to share this information and guidance with the relevant stakeholders.

To share, provide or arrange online safety advice and training, where necessary, for all staff, parents and carers and governors.

To liaise closely with the Headteacher and report all safeguarding issues accordingly.

Security and Data Management:

IT security is a shared responsibility and involves all users of technology within the school. The school follows guidance and security standards provided by Lancashire County Council and other relevant bodies and ensures that information and personal data are processed securely and in accordance with the UK GDPR, the Data Protection Act 2018 and associated statutory guidance.

Acceptable Use of Devices including Wearable Technology:

Pupils

At school we use school-owned mobile devices including laptops, tablets, mobile phones, cameras and games consoles to provide enriching learning opportunities for our children. Children will only use such devices in the presence of an adult.

In line with the latest DFE guidance, Great Arley School is a mobile phone-free environment. Pupils must not use or access mobile phones, smart watches or other personal smart devices at any time during the school day, including before registration, during lessons, transitions, breaktimes and lunchtimes, unless an exception has been agreed in advance by the Headteacher or Deputy Headteacher.

Where a pupil brings a mobile phone or smart device onto the school site, it must be secured in a school-approved locking pouch for the duration of the school day and must not be accessed by the pupil. Any unauthorised use of, or access to, a mobile phone or smart device will result in the device being confiscated, parents or carers being informed, and the school reviewing whether the pupil will continue to be permitted to bring the device into school.

Where a mobile phone or smart device is required to meet a pupil's assessed medical needs, appropriate arrangements will be agreed, documented and reviewed by the designated safeguarding lead.

Staff, Governors, Volunteers and all Visitors

All staff, governors, volunteers, contractors and visitors must ensure that mobile phones and personal electronic devices are stored securely and remain inaccessible to pupils when not in use.

Personal electronic devices, including mobile phones, smart watches, smart glasses and other wearable technology with communication, recording or image-capturing capabilities, must not be used in areas accessed by pupils unless there is an exceptional and authorised operational requirement. Prior authorisation must be obtained from a member of the Senior Leadership Team (SLT). Any authorised use must be proportionate, time-limited, necessary for the purpose intended and compliant with the school's safeguarding and data protection policies.

Where smart wearable devices are worn on the school site, all camera, recording, messaging, voice-calling and communication functions must be disabled. Such devices must not be used to take photographs, make audio or video recordings, send or receive messages, access emails, social media, internet content or personal notifications during working hours or whilst undertaking duties on behalf of the school.

Smart wearable devices must not be worn during intimate care, personal care, toileting, changing, hydrotherapy, swimming activities, first aid, medical treatment or any activity where pupils have an increased expectation of privacy, dignity or confidentiality.

Staff are responsible for ensuring that any personal electronic device or wearable technology brought onto the school site complies with these requirements. Failure to do so may be treated as a breach of the school's safeguarding procedures, staff code of conduct, acceptable use agreement and may result in management action being taken.

Personal electronic devices, including school-issued devices, must not be used in areas where intimate care, personal care or medical procedures are taking place unless their use is required for an authorised educational, operational, safeguarding or medical purpose and appropriate safeguards are in place.

Staff, governors, volunteers, and visitors must not use personal mobile phones or personal electronic devices in the presence of pupils. Personal devices must never be used to take photographs, videos or audio recordings of pupils under any circumstances. Where images or recordings of pupils are required for educational or operational purposes, only school-authorised devices may be used and only in accordance with the school's safeguarding, consent and data protection procedures.

Where contractors or external professionals are required to use a personal mobile phone or device in connection with work being undertaken on behalf of the school, this must be authorised and supervised by a member of the Senior Leadership Team or a designated senior member of staff. Use of personal devices should be limited to work related purposes, such as completing electronic forms, accessing work documentation, recording job information, or taking photographs directly related to maintenance, repairs, inspections or other contracted works.

Wherever possible, such activities should be carried out when pupils are not present; however, we recognise that this may not always be practicable. In these circumstances, all reasonable precautions must be taken to avoid capturing, viewing or recording pupils or their personal information. Any photographs taken must be strictly necessary for the work being undertaken and will be checked immediately by the supervising senior member of staff to ensure no pupils or identifying information are visible. Where an image inadvertently includes a pupil, the image must be deleted immediately and permanently in the presence of the supervising member of staff.

Personal use of mobile phones during the school day (8.45am to 3.30pm) is permitted only within the designated staff areas identified in Appendix 2 and must not interfere with the supervision, care, welfare or education of pupils.
Staff, governors and volunteers must ensure that personal devices are switched to silent mode during the school day. Visitors must ensure that mobile phones and personal electronic devices are switched off whilst on the school site.

Where staff are authorised to contact parents or carers using a personal device, communication must take place only through the school's approved communication platform, the **Linkus App**. Staff must not use personal telephone numbers, messaging services, social media platforms or personal email accounts to communicate with parents or carers regarding school matters. A written record of all communications made through the Linkus App must be maintained in accordance with school procedures, and any communication relating to safeguarding, welfare, behaviour or wellbeing concerns must be recorded on CPOMS without delay.

Use of Cameras and Recording Devices:

The guidance below is taken from the school's Safeguarding and Child Protection Policy and must be followed.

For the purpose of this document a camera refers to any mobile device which can take a picture.

Consent

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the school seeks and records parental consent for the taking and use of photographs and recordings for the purposes outlined below. Parents and carers are reminded annually to notify the school of any changes to their consent preferences. Responsibility for informing the school of any changes to consent rests with the parent or carer.

Staff are advised to check this consent before taking and using photographs and recordings of pupils. The staff in the school office hold an up-to-date list of pupils who are prohibited from having their photograph used for any purpose other than within school for example the school website, social media or wider media contexts.

Purpose of Photographs/ Video

Children throughout school might have their photographs taken by staff to:

- Provide evidence of progress for moderation, developmental records and recording pupil's work;
- Celebrate their achievements e.g. for displays in school.
- Create guidance notes e.g. for care plans or behaviour plans.

In addition, photographs may be used to advertise or promote the school via the website, social media platforms, newspaper reports and the school prospectus. The school seeks parental consent to take photographs or recordings for these purposes.

When pupils are working together any photographs taken may contain other children in the background. Staff need to be aware of this and check parental consent before using the photographs.

When pupils are in photographs which are used for external accreditation and may need to be sent to examination boards for moderation purposes, the school will seek specific consent to send photographs or recordings for this purpose.

Specific permission will be sought from parents and carers for images of pupils used on individual communication aids which may go home with a child.

All photographs must be taken on school-owned devices; no one is permitted to use their own mobile phones, cameras or recording devices. Staff, visitors, volunteers and pupils are not permitted to use their own mobile phones or cameras or other recording devices to take or record any images of children for their own records during school time.

The school-owned devices must not leave the school setting unless on an educational visit.

Parents and Carers

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, parents and carers may be permitted to take photographs or recordings of their own child during school events, subject to the school's safeguarding and privacy requirements. Parents and carers must, as far as possible, focus images and recordings on their own child and must not share photographs or recordings containing other pupils on social networking sites or other public platforms without the appropriate consent.

Parents and carers may only take photographs or recordings when authorised by the school and in the presence of staff. The school reserves the right to prohibit photography or recording at any event where safeguarding, privacy or welfare concerns arise.

Parent volunteers must not use personal mobile phones or personal electronic devices to take photographs, videos or recordings of pupils whilst undertaking volunteering activities, including educational visits and school trips. Where photographs are required for educational purposes, only school-authorised devices may be used in accordance with the school's safeguarding, consent and data protection procedures.

The Press

The press have special permissions in terms of data protection and may wish to name individual children to accompany a photograph this will only be allowed with written permission gained from parents. Each time a photograph is to be used as a press release; confirmation of permission will be sought prior to photographs going to press.

Storage and use of pupil information including photographs/ video:

School

Images of pupils are stored in a range of places, for example share point, one drive or on an individual school device. All school devices are password protected and encrypted in line with the school's ICT service provider.

Cyber Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by the ICT service provider (Comptech) to help them store their passwords securely. Teachers will keep pupil's passwords in a secure location in case pupils lose or forget their passwords.

Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the school's ICT supplier (Comptech).

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the School Business Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider (Comptech).

Photographs must be deleted when no longer required and as a guide this will be at the end of a key stage or when a child leaves the school.

Printing can only be done in the school setting. Individual printed photographs will remain in school until no longer required by school or sent home to the parent of the child who is depicted in the photograph. Photographs must be deleted and any printed copy must be destroyed.

Cameras, mobile phones and all types of recording devices are prohibited in changing or toilet areas.

There is one school mobile phone, which has a camera as standard; this is located in the school office. This phone is to be taken by a member of staff on all visits out of school. They will have the school office number entered into the phone. These phones are for emergency contact with school, staff on the visit, parents and carers or the emergency services only.

If there is an allegation made against a member of staff regarding the use of mobile phones, cameras or other recording devices, the LCC procedures for *Managing Allegations against Staff* will be followed. **(Great Arley School Safeguarding and Child Protection Policy)**

When taking photographs all staff must maintain the dignity of the pupils; they should ensure that pupils are happy to be photographed and that they are suitably dressed and presented. All photographs must show pupils in a positive light.

Communication Technologies:

Email

Microsoft Outlook is the school email system. Personal email accounts should not be accessed in school time on school equipment.

All children in KS3 & 4 have their own school email account as part of planned curriculum activities. Pupils using email accounts are always supervised by staff. As part of PSHE and Computing pupils are taught about the issues associated with use of e-mail and cyber-bullying.

All users must be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act. Pupils will be taught how to use the email safely and what to do if cyber-bullying occurs. (refer to the Safeguarding and Child Protection policy).

Social Networks

Great Arley recognises that social networking and social media platforms can provide valuable opportunities for communication, learning and professional development. However, their use can also present safeguarding, privacy and reputational risks.

Pupils, staff, governors, volunteers and visitors are expected to use social networking sites, messaging services and online platforms responsibly, safely and lawfully.

Pupils must not engage in behaviour online that could place themselves or others at risk, including cyberbullying, harassment, sharing inappropriate content or disclosing personal information.

Staff, governors and volunteers must maintain appropriate professional boundaries at all times and must not communicate with pupils through personal social networking accounts, messaging services or other non-approved platforms. Personal social media use must not compromise the confidentiality, welfare or safety of pupils, colleagues or the school community. Any concerns relating to online behaviour, cyberbullying, inappropriate content, online exploitation or breaches of professional conduct must be reported promptly in accordance with the school's safeguarding and behaviour procedures.

All use of social media must comply with the school's safeguarding, online safety, staff code of conduct, acceptable use, data protection and confidentiality requirements, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the expectations set out in Keeping Children Safe in Education.

The safe and professional use of social networking forms part of staff induction and ongoing safeguarding training. When using social networking sites, all members of staff must conduct themselves in a professional manner and recognise that content published online may be permanent, publicly accessible and capable of being shared beyond its intended audience.

Staff who use social networking sites in a personal capacity must not share personal contact details, including telephone numbers, personal email addresses, social media profiles, blogs or websites, with pupils or parents/carers.

Privacy settings should be reviewed regularly to minimise the risk of personal information being accessed by others.

Online content must not bring the school into disrepute, undermine public confidence in the school, breach confidentiality, damage professional relationships or be derogatory towards pupils, colleagues, parents/carers or the wider school community.

Staff must not communicate with current pupils, former pupils under the age of 18, or siblings of pupils through personal social networking accounts, nor should they accept or initiate 'friend' requests or similar connections. Guidance for staff regarding appropriate online conduct is provided in Appendix 3.

In accordance with safer recruitment requirements set out in Keeping Children Safe in Education, the Senior Leadership Team will undertake online searches on shortlisted candidates as part of the recruitment process. These searches will be conducted fairly, consistently and in accordance with the school's recruitment procedures. Information obtained will only be considered where it is relevant to an applicant's suitability to work with children and young people and will be processed in accordance with data protection legislation.

School Use of Facebook

The school has a Facebook and account, details of which can be found in the appendix. This is used to share information and events with the community. This school Facebook page is a public account. The sharing of pupil consent is covered by our parental consent protocols.

Curriculum

Our PSHE and computing curriculums both cover the acceptable use of social networking sites, emails and text messaging. We regularly discuss the safe and acceptable use of such communication technologies in school, and we invite our local PCSO into school to keep our pupils updated on the law governing these.

All pupils will be educated in the safe use of social networking.

Instant Messaging or VOIP

Instant messaging systems, e.g. text messaging, facetime, Teams etc are popular communication tools with both adults and children. Staff and pupils must not use school equipment to communicate with personal contacts e.g. through facetime on an iPad. Internet content filtering is provided by default by Education Digital Services, Netsweeper.

The school successfully uses Parent App to communicate with parents. All messages are sent via a notification on the app, text or email. All data is safely stored within SIMS and is synced at regular intervals.

School administration staff, under supervision of the Headteacher and Deputy Headteacher are the only staff who can access the Parent App service.

Websites and Other Online Publications

This may include for example school websites, Social Network profiles, podcasts, videos, wikis and blogs. Information posted online is readily available for anyone to see and thus form an opinion about the school. Our school website communicates Online Safety messages to parents/carers. The website is only edited by administration staff and in agreement with the Headteacher or Deputy Headteacher.

Content is regularly reviewed by the Headteacher who has overall responsibility for what appears on the website.

Downloadable materials are in a read-only format (e.g. PDF)

Written consent from parents and carers for photographs of their children used on the web site is obtained.

Infrastructure and technology including filtering and virus protection:

The school ensures that the infrastructure and network are as safe and secure as possible by subscribing to Education Digital Services (EDS).

Internet content filtering is provided by default by EDS (Netsweeper). It is important to note that the filtering service offers a high level of protection. Pupils have restricted access provided by the filter. Staff also have restricted access via Netsweeper filtering, however their permissions are elevated by our IT provider to allow unrestricted access to certain sites. It is vital therefore that staff do not allow pupils access to their log-in details or leave their computer logged-in and left unattended.

Sentinel One Anti-Virus software is installed on all computers and laptops in school and then configured to receive regular updates.

If any unsuitable content gets past the filter service, it must be reported to the DSL and SLT and recorded as a serious incident on CPOMS.

The school subscribes to OnGuard through Lancashire County Council's Broadband service. This is a monitoring and alerting service designed to alert key staff members if students/ staff are accessing unlawful materials on line. The system is able to alert key members of staff in real time if an area of concern is identified. If the concern is considered a threat to life then the school will receive a phone call alerting the DSL to the situation.

Pupil Access

Pupils are always supervised by a member of staff when accessing school digital equipment and online materials. They are taught about safe use of equipment and keeping safe on-line at school and at home. Pupils are taught the procedure to follow if they unwittingly view inappropriate content whilst online. Pupils who purposefully view inappropriate content will be subject to the school's discipline procedure, outlined in the *Behaviour Policy*. Any incidents are recorded as a serious incident on CPOMS.

Managing the Network and Technical Support

The school works in partnership with Education Digital Services and our external IT support provider to ensure that the systems to protect pupils are reviewed and improved. The monitoring of the internet content accessed by pupils takes place weekly, by the DSL.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP. See the Online Safety Incident Escalation/ Procedure (APPENDIX 4)

Internet Watch Foundation (IWF)

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Always report potentially illegal content to the Internet Watch Foundation http://www.iwf.org.uk. They are licensed to investigate – schools are not!

Examples of illegal offences are:

Accessing child sexual abuse images.

Accessing non-photographic child sexual abuse images

Accessing criminally obscene adult content.

Incitement to racial hatred.

Accidental Access to Inappropriate Content.

If any inappropriate content is accidentally accessed, then the procedures to be followed are outlined in the Online Safety Incident Escalation/ Procedure (APPENDIX 4). Briefly:

Staff - Minimise the webpage/turn the monitor off. Report to DSL, record all details on CPOMS.

Child- Minimise the web page/turn off the monitor and tell an adult immediately.

Acceptable Use for all Stakeholders:

Education and Training:

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond including how to respond to cyber-bullying and incitement to racial hatred.

At Great Arley we teach this through our differentiated PSHE curriculum; our Computing curriculum; by staff continuously acting as a role model for pupils and by regularly referring to Online Safety when pupils are using digital technology. This is also personalised to the individual needs of pupils where necessary through Online Safety guidance if an incident occurs and it may form part of a pupil's PLG, if an identified need is recognised. We also hold a focused whole school Online Safety Day and assembly held in conjunction with national online safety initiative. We also have an annual focussed anti-bullying week held in conjunction with The Anti-Bullying Alliance awareness week in the autumn term. This addresses aspects of online safety, including cyber-bullying.

We share online safety materials, especially those pertaining to current local and national issues, with parents and carers through the school website and Parent App. We reinforce with parents and carers the importance of monitoring online behaviour and reporting incidents and offer support in setting parental controls on devices and how to support their children in assessing risk whilst online.

Our *Online Safety and Acceptable Use Policy* is available on our school website or hard copies can be obtained from the school office on request.

There are some useful websites which stakeholders can refer to for various online safety guidance (listed below):

Online Safety for Schools | SWGfL

Keep Children Safe Online: Information, advice, support - Internet Matters

CEOP Safety Centre

Eliminating Child Sexual Abuse Online | Internet Watch Foundation IWF

Home | Better Internet for Kids

Use of Artificial Intelligence (AI)

See Generative AI policy

Online Safety – Raising Staff Awareness:

New staff and volunteers are inducted in the safe use of technology and are sign posted to this policy.

Online Safety – Governors:

Governors are part of our commitment to online safety.

The *Online Safety and Safeguarding Policies* are reviewed regularly according to the school's policy monitoring cycle and are discussed at the governors' committee meetings.

Governors receive specific online safety training delivered through school or the Local Authority Governor Services.

There is a requirement that governors with lead/ link roles and responsibility for child safeguarding - Mrs H Williams, will attend training courses provided by the LA and keep up to date with developments.

Evaluating the Impact of the Online Safety and Acceptable Use Policy:

The Online Safety and Acceptable Use Policy will be reviewed annually according to the school's policy monitoring cycle or when an incident occurs that deems it necessary.

The Safeguarding Governor, DSL and Headteacher will monitor incidents termly to check for any recurring patterns emerging and action accordingly. This policy will be amended as necessary.

Great Arley School – Appendix 1

Acceptable Use Agreement for Pupils - Key Stage 1 & 2

When I use the school IT equipment or go online at home or at school:

I will only send polite and kind messages to others.

I will not tell anyone my password.

I will look after the equipment.

I will ask for help if I don't know what to do.

I will only use equipment to do the work my teacher has set for me.

I will only take a picture or video of other people if they say it is OK.

I will tell my teacher if I see something that makes me worried or unhappy.

I know that my teacher can see my work and if I break the rules I might not be allowed to go online or use the IT equipment for a while.

Great Arley School – Appendix 1

Acceptable Use Agreement for Pupils - Key Stage 3 & 4

My school provides IT equipment and access to the Internet to support my learning and help me to communicate with my teacher and peers. I have certain responsibilities when using digital technologies at home as well as at school.

I agree to the following rules:

I will use the school's IT equipment safely and responsibly.

I will keep my password private and not share it with others.

I will never use someone else's login details or send messages pretending they are from someone else.

I will report any suspicious communications, instances of cyberbullying or inappropriate material immediately.

I will never copy someone else's work and use it as my own.

I will never use AI generated text or imagery and use it as my own.

I will only post polite, positive and kind messages online.

I will not post fake information online.

I will not share personal information, including photos online or use GPS to disclose my location.

I will never take or post photos or videos of others without their permission.

I will not bring personal digital devices to school unless I have been given permission to do so.

I will not search for inappropriate material online or share any such material with others.

I will use school equipment and the Internet to complete work set by my teacher and not for anything else.

I understand that the school will monitor my use of digital technologies and that, if I do not follow these rules, my access to the Internet and digital technologies may be stopped for a period of time

Appendix 1

Acceptable Use of the Internet: Agreement for Parents and Carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page (the messenger facility is not monitored) • Parent App • Class Dojo • Evidence for Learning • Email
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Appendix 1

Acceptable Use of the School's ICT Facilities and the Internet: Agreement for Staff, Governors, Volunteers and Visitors

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and School Business Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

APPENDIX 2

List of places where staff are permitted to use personal mobile phones during the school day.

Off site

Staffroom

SLT office

School office

Kitchen office

Site Supervisors' office

PPA room with door closed

Appendix 3

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

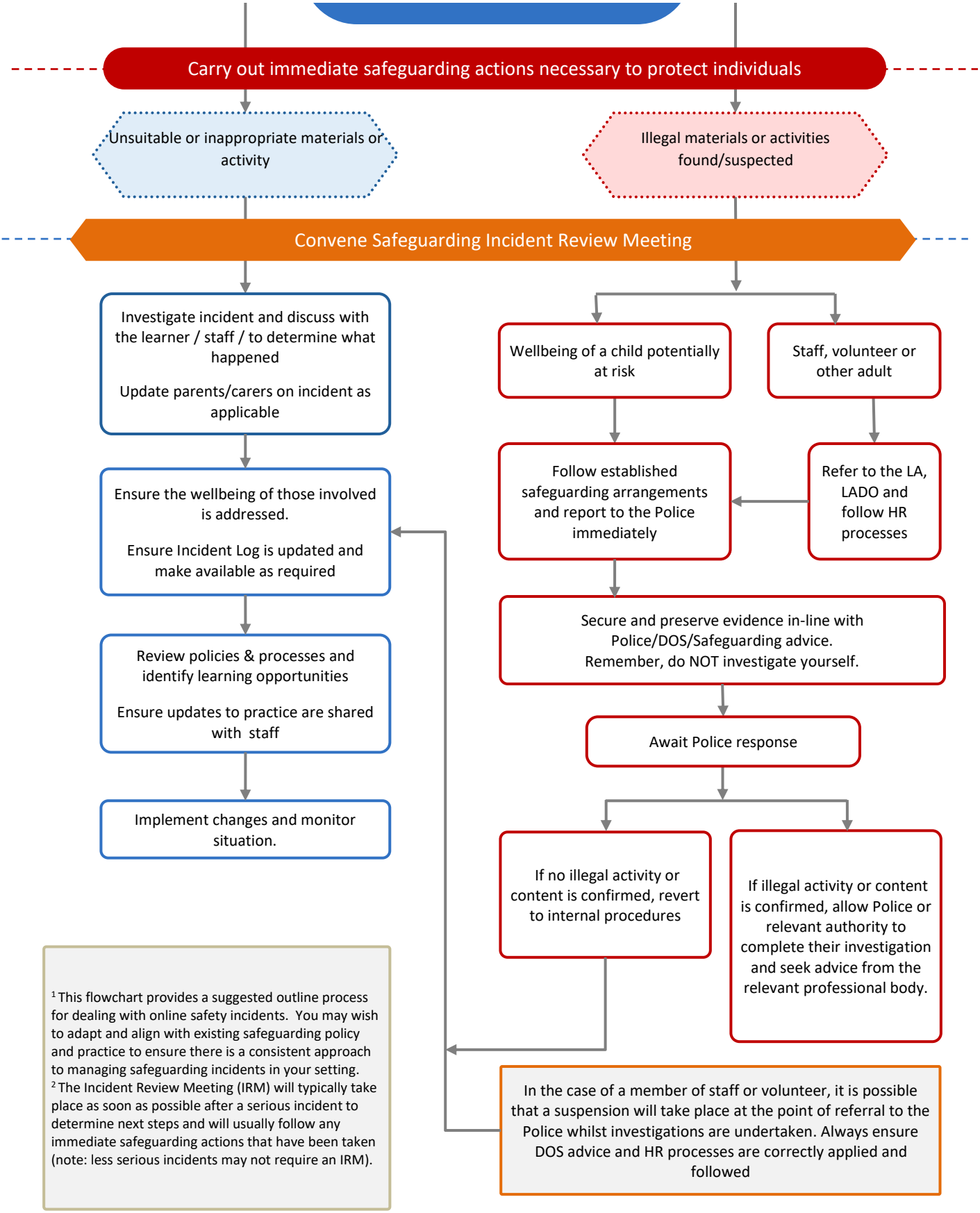
- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

APPENDIX 4

Online Safety Incident Escalation/ Procedure



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).