Alma Primary Digital-Safety Policy

Responsibility:	*Marc Shoffren*
Governor responsible:	*Louise Lewis*
Last review date:	*January 2023*
Next review date:	*Spring 2025*

Contents

Policy Development: new – amended

Change	Responsible	Date
Updated to Digital-safety & added use of internet section	MJS	April 2018
Full policy update	D Davies	Jan 2023

1 Aims

1.1 Alma Primary understands that using online communication and digital technology ("online services") are important aspects of raising educational standards, promoting child achievement and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of children and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.2 At Alma Primary we aim to use online services to enhance learning and teaching across the curriculum. We recognise that, as with any tools, the use of technology comes with potential hazards, and so this policy aims to create a framework to support teaching and address such hazards by:

- Providing reasonable safeguards to support learning;
- Reminding all members of the learning community of their roles and responsibilities in regard to online and digital-safety;
- Ensuring adequate monitoring and reporting of online and digital-safety incidents;
- Creating a framework to address typical problems which may arise from the use of online services at alma primary.

2 Legal framework

2.1 This policy has due regard to all relevant legislation and guidance including, but not limited to:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (GDPR) and Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000

- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of children Act 1978
- Protection from Harassment Act 1997

2.2 This policy should be read in conjunction with the following school policies:

- Alma Allegations of Abuse Against Staff Policy
- Alma Acceptable Use Agreements
- Alma Behaviour for Learning Policy
- Alma Data Protection Policy and Alma Data Security Incident Response Policy
- Alma Safeguarding Policy
- Alma Preventing Bullying Policy
- Alma PSHE and Wellbeing Policy
- Alma Staff Code of Conduct
- Alma Staff Disciplinary Policy

3 Scope of the Policy

3.1 This policy applies to all members of the Alma Primary community, including staff, children, volunteers, parents / carers, visitors, community users and any other individuals who have access to and/or are users of the school's ICT systems and/or online services, both in and out of the school.

3.2 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other digital-safety incidents covered by this policy, which may take place outside of the school, but are linked to children and staff. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's policies.

3.3 The school will deal with such incidents in line with its policies and government guidance and, where appropriate, inform relevant parents / carers of incidents of inappropriate digital-safety behaviour that take place inside and outside of school.

4 Roles and Responsibilities

The following section outlines the digital-safety roles and responsibilities within the school:

4.*1* ***Digital-Safety Coordinator:*** The Digital-Safety Coordinator, in conjunction with the Designated Safeguarding Lead (DSL), is responsible for day-to-day digital-safety. These responsibilities include:

- Reviewing the school's Digital-Safety policy and relevant documentation;
- Day-to-day digital-safety issues;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of a digital-safety incident occurring;
- Providing training and advice for staff;

- Liaising with the relevant local and national bodies;
- Liaising with school ICT technical staff (whether directly employed or under contract);
- Maintaining a log of digital-safety incidents to inform future digital-safety developments;
- Meeting regularly with the Digital-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- Reporting regularly to the School Leadership Team;
- Liaising with the DSL
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day;
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff;
- Ensuring that all members of the school community understand the reporting procedure;
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns;
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures;
- Reporting to the governing board about online safety on a termly basis.
- Working with the Headteacher and ICT technicians to conduct termly light-touch reviews of this policy;
- Working with the headteacher and governing board to update this policy on an annual basis;
- Attending relevant meetings held by the Learning and children Committee.

4.2 The DSL is responsible for:

- Taking the lead responsibility for online safety in the school;
- Acting as the named point of contact within the school on all online safeguarding issues;
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with send face online;
- Liaising with relevant members of staff on online safety matters, e.g. Digital-safety coordinator and ict technicians;
- Ensuring that online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented;
- Ensuring that safeguarding is considered in the school's approach to remote learning;
- Ensuring that appropriate referrals are made to external agencies, as required;
- Working closely with the police during police investigations;
- Keeping up-to-date with current research, legislation and online trends.

4.3 *ICT Technical staff:* Any ICT Technical Staff employed or contracted by Alma Primary are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack;
- The school meets all digital-safety technical requirements and any relevant local or national body digital-safety guidance that may apply;
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- Appropriate filtering is applied and updated on a regular basis, and that its implementation is not the sole responsibility of any single person;

- They keep up to date with digital-safety technical information in order to effectively carry out their digital-safety role and to inform and update others as relevant;
- The use of the network and any technical systems used by the school, including email and cloud-based storage and facilities, are regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher and/or digital-safety coordinator for investigation and action where appropriate;
- Monitoring systems are implemented and updated regularly.

4.4 *All Teaching and Support Staff:* All staff, including School Leaders and members of the administration and support teams are responsible for ensuring that:

- They have an up to date awareness of digital-safety matters and of the current school digital-safety policy and practices;
- They have read, understood and signed the staff acceptable use agreement;
- They report any suspected misuse or problem to the headteacher, DSL and/or digital-safety coordinator for investigation, as required and in accordance with school policy;
- All digital communications with parents / carers and, when relevant, children, should be on a professional level and only carried out using official school systems;
- Digital-safety issues are embedded in all aspects of the curriculum and other activities;
- Children understand and follow the digital-safety and acceptable use policies;
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor the use of online services, 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, children are guided to sites which have been checked as suitable for their use, and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.5 *Headteacher and School Leaders:* In addition to the responsibilities for all staff, noted above, the Headteacher of Alma Primary has responsibility for:

- The overall safety (including digital-safety) of members of the school community;
- Ensuring that regular monitoring reports are received from the digital-safety coordinator;
- Ensuring that the digital-safety coordinator and other relevant staff receive suitable training to enable them to carry out their digital-safety roles and to train other colleagues, as relevant;

4.6 *Children:* At Alma Primary children are taught about:

- Using the school's online services in accordance with the Student Acceptable Use Policy;
- Research skills and the need to avoid plagiarism and uphold copyright regulations;
- The importance of reporting abuse, misuse or access to inappropriate materials, and knowing how to do so;
- The school's policies on the use of mobile devices and online services;
- School policies on the taking or using images, and on cyberbullying;
- The importance of adopting good digital-safety practice when using online services out of school, that the school's Digital-Safety Policy covers their actions outside of school, if related to their membership of the school.

4.7 *Parents / Carers:* Parents and/or carers play a crucial role in ensuring that their children understand the need to use the internet and technology in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website links and information about national or local digital-safety campaign. Parents and carers are encouraged to support Alma Primary in promoting good digital-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- Access to parents' sections of the website and on-line children' records;
- Their children's personal devices in the school (where this is allowed).

4.8 *Governors:* Governors are responsible for the approval of the Digital-Safety Policy and for reviewing the effectiveness of the policy. This responsibility will be held by the Learning and children Committee, who will receive termly monitoring updates, including information about digital-safety incidents. The governor responsible for safeguarding is also the designate Digital-Safety Governor. The role of the Digital-Safety Governor will include:

- Regular meetings with the Digital-Safety Coordinator;
- Regular monitoring of digital-safety incident logs;
- Ensuring that appropriate filtering is in place;
- Reporting to the Learning and children Committee on a termly basis and to the Governing Body on an annual basis;
- Ensuring their own knowledge of online safety issues is up-to-date.

4.9 *Community Users:* Community Users who access the school's technology systems and resources as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school technology, with the exception of access to the school wifi. Use of any school facilities is contingent on the community users adhering to the agreement. Any infringement of the agreement my result in the community user being barred or restricted from using any of the school's facilities, whether technology related or not.

5 Managing Online Safety

5.1 Integration of Online Safety. All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive training in INSET and staff briefings;
- Staff receive email updates regarding online safety information and any changes to online safety guidance or legislation;
- Online safety is integrated into learning throughout the curriculum;
- Assemblies are conducted regularly on the topic of remaining safe online.

5.2 Reporting of online safety concerns. Any disclosures made by children to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the school's Safeguarding Policy. Staff should be aware

that children may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff should be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also understand that children displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. All staff, and in particular the DSL, will act in accordance with school policies (such as the Safeguarding Policy), legislation and training, with the victim's best interests at the centre of decision making.

The school may choose to avoid unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a child has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the school's Safeguarding Policy. All online safety incidents and the school's response must be recorded by the DSL.

5.3 Reporting specific incidents. Whereby a staff member is required to report a safeguarding incident relating to a child, this should be reported to the DSL via CPOMs (except where the concern also relates to the Headteacher, in which case it must be reported to the Chair of Governors). If the matter is not a potential safeguarding concern relating to a child, it should be reported to the Headteacher, if the concern is about any other staff member, and to the Digital Safety Coordinator in all other circumstances.

5.4 Where a child is required to report an incident involving the use of online services at school, this may be directed to any staff member. Following receipt of such a report, the staff member should report any concerns to the Headteacher, Designated Safeguarding Lead and/or Digital Safety Coordinator as per 5.3 above.

5.5 If there is any suspicion that a website containing child abuse images may have been accessed, if there is any other suspected illegal activity relating to the use of technology or internet at school, or it is suspected that unsuitable online material may have been accessed at school, the Online Safety Incident flowchart (Appendix 6) should be followed by the Headteacher or person(s) appointed by the Headteacher.

5.6 In all circumstances, proper regard should be given to other school policies as above (including but not limited to the Safeguarding Policy, Acceptable Use Agreement and Staff Code of Conduct).

6 Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages;

- Threatening or embarrassing pictures and video clips sent via mobile phone cameras;
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Unpleasant messages sent via instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook;
- Abuse between young people in intimate relationships online i.e. Teenage relationship abuse;
- Discriminatory bullying online i.e. Homophobia, racism, misogyny/misandry.

The school is aware that certain children may be more at risk of abuse and/or bullying online, such as LGBTQ+ children and children with SEND. Cyberbullying against children or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the school's Anti-bullying Policy.

7 Child-On-Child Sexual Abuse and Harassment

7.1 Children may also use the internet and online services as a vehicle for sexual abuse and harassment. Staff understand that this abuse can occur both in and outside of school, off and online, and are aware that children are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age. The following are examples of online harmful sexual behaviour of which staff are aware:

- Threatening, facilitating or encouraging sexual violence;
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks;
- Sexualised online bullying, e.g. sexual jokes or taunts;
- Unwanted and unsolicited sexual comments and messages;
- Consensual or non-consensual sharing of sexualised imagery;
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

7.2 All staff are aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff are aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to children becoming less likely to report such conduct.

7.3 Staff are aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

7.4 The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse must be reported to the DSL, who will investigate the matter in line with the school's Safeguarding Policy.

8 Grooming and exploitation

8.1 Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them. Staff are aware that grooming often takes place online and that children who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The child believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger, with the intention of gaining their trust to abuse them;
- The child does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life;
- The child may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family;
- Talking to someone secretly over the internet may make the child feel 'special', particularly if the person they are talking to is older;
- The child may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

8.2 Due to the fact children are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. These may include:

- Being secretive about how they are spending their time;
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met;
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

8.3 **Child sexual exploitation (CSE) and child criminal exploitation (CCE).** Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

8.4 Where staff have any concerns about children with relation to CSE or CCE, they must bring these concerns to the DSL without delay, who will manage the situation in line with the school's Safeguarding Policy.

8.5 **Radicalisation.** Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

8.6 Staff members are aware of the factors which can place certain children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff are expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised. Where staff have a concern about a child relating to radicalisation, this must be reported to the DSL without delay, who will handle the situation in line with school policy.

9 Mental health

9.1 The internet, particularly social media, can be the root cause of a number of mental health issues in children, e.g. low self-esteem and suicidal ideation. Staff are aware that online activity both in and outside of school can have a substantial impact on a child's mental state, both positively and negatively. Concerns about the mental health of a child will be dealt with in line with school policy on PHSE and Wellbeing.

10 Online hoaxes and harmful online challenges

10.1 For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the child and the way in which they are depicted in the video.

10.2 Where staff suspect there may be a harmful online challenge or online hoax circulating amongst children in the school, they must report this to the DSL immediately. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to children, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the Local Authority and/or other appropriate authorities about whether quick local action can prevent the hoax or challenge from spreading more widely.

10.3 Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. The UK safer internet centre, when fact-checking the risk of online challenges or hoaxes;
- Careful to avoid needlessly scaring or distressing children;
- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. Where content is explained to younger children but is almost exclusively being shared amongst older children;
- Proportional to the actual or perceived risk;
- Helpful to the children who are, or are perceived to be, at risk;
- Appropriate for the relevant children' age and developmental stage;

- Supportive;
- In line with the school's safeguarding policy.

10.4 Where the DSL's assessment finds an online challenge to be putting children at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, the DSL will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.
The DSL and headteacher may also implement a school-wide approach to highlighting potential harms of a hoax or challenge, having considered the risk of increasing children' exposure to the hoax or challenge, and examined ways in which this risk may be mitigated as far as possible.

11 Cyber-crime

11.1 Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

11.2 The school factors into its approach to online safety the risk that children with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

12 Digital-Safety Education of children

12.1 The education of children in digital-safety is an essential part of the school's digital-safety provision. children need the help and support of the school to recognise and avoid digital-safety risks and build their resilience.

12.2 Digital-safety should be a focus in all areas of the curriculum and all staff should reinforce digital-safety messages across the curriculum. Teaching about digital-safety should be broad, relevant and provide progression, with opportunities for creative activities, and should be delivered through the following methods:

- A computing curriculum which includes strong elements of specified digital-safety, provided as part of the school's main curriculum, that is regularly revisited, at least on an annual basis;
- Key digital-safety messages should be reinforced as part of a planned programme of assemblies;
- Children should be taught in all relevant lessons to be critically aware of the materials / content they access on-line, and be guided to validate the accuracy of information;

- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Children should be helped to understand the need for the acceptable use agreement, and encouraged to adopt safe and responsible use of technology both within and outside school;
- Staff should act as good role models in their use of online services and mobile devices;
- In lessons where internet use is pre-planned, children should be guided to sites previously checked as suitable for their use, and that processes should be in place for dealing with any unsuitable material that is found in internet searches;
- Where it is deemed appropriate, older children may use unguided, free searching, provided that adequate supervision arrangements are in place and the teacher is aware of strategies for dealing with inappropriate or unsuitable sites that may be encountered;
- It is accepted that, from time to time, for good educational reasons, children may need to research topics (e.g. Racism, drugs, discrimination) that would normally result in internet searches being blocked through web-filtering. In such circumstances, staff may request that those sites are temporarily removed from the filtered list, for the period of study. Any request for this provision should be auditable, with clear reasons given for the temporary change. Appropriate safeguards should be implemented to protect all children (including those in other classes) during periods of temporary changes to web-filtering;
- The school recognises that, while any child can be vulnerable online, there are some children who may be more susceptible to online harm or have less support from family and friends in staying safe online, such as children with special educational needs and 'looked after' children. Relevant members of staff such as the senco and learning support assistants will support the class teacher in adapting the curriculum to ensure that all children receive the information and support they need.

13 Digital-Safety Education of Staff

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

- Digital-safety training will be made available to staff as part of the school's INSET training programme;
- All new staff should receive digital-safety training as part of their induction programme, ensuring that they fully understand the school's Digital-Safety Policy and Acceptable Use Agreements;
- The Digital-Safety Policy and its updates will be shared with staff and discussed in staff team meetings or briefings;
- Where possible, training will help staff to identify and act on behaviours which give rise to concerns, including behaviour which may indicate the potential grooming or abuse of a child;

14 Digital-Safety Education of Governors

14.1 Governors should take part in digital-safety training sessions, with particular importance for those who are members of any sub-committee / group involved in technology and child safeguarding. This may be through:

- Attendance at training provided by the local or national organisations;
- Participation in school training for staff or parents;
- Whole governing body training.

15 Digital-Safety Education of Parents / Carers

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

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

- Curriculum activities;
- Direct communication to parents / carers;
- Indirect communication (such as via the school website);
- Parents / carers evenings / sessions;
- High profile events / campaigns eg. Safer internet day;

16 Equipment, filtering and monitoring

16.1 The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy document are implemented. The school will ensure that the relevant parties referenced in the above sections of this document are effective in carrying out their digital-safety responsibilities. To this end, the school will ensure that:

- Technical systems are managed in appropriate ways, agreed with the school's ICT provider and technical support team;
- There are regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users have clearly defined access rights to school technical systems and devices;
- Users are provided with a username and secure password (where appropriate and dependent on the age of the user), and the school keeps an up to date record of users and usernames. Users are responsible for the security of their username and password and will be required to change their password regularly;
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other authorised persons) must also be available to the Headteacher or other nominated Senior Leader, and kept in a secure location;
- 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, as deemed appropriate, in particular that Illegal content (such as child sexual abuse images) is filtered by the broadband or filtering provider and by the school's own filtering system;
- Filter 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;
- The school has differentiated user-level filtering (allowing different filtering levels for different classes and different groups of users);
- School ICT technical staff monitor the activity of users on the school technical systems;
- An appropriate system is in place for users to report any actual / potential technical incident or security breach to the digital-safety Coordinator;
- 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, that these are tested regularly, and that

the school infrastructure and individual workstations are protected by up to date virus software;
- A system policy is in place for the provision of temporary access of "guests" (e.g. Trainee teachers, supply teachers, visitors) onto the school systems);
- A system policy is in place regarding the extent of personal use that users (staff / children / community users) and their family members are allowed on school devices that may be used out of school;
- A system policy is in place that prohibits staff from downloading executable files and installing programmes on school devices.

16.2 *Use of Digital and Video Images:* The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the internet. Digital images uploaded to the internet may be duplicated beyond the control of users and/or the school, with the potential to cause harm or embarrassment to individuals in both the short or longer term. The school will inform and educate users about these risks and will implement the following guidance to reduce the likelihood of potential harm:

- When using digital images, staff should inform and educate children 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 site;
- In accordance with guidance from the information commissioner's office, parents / carers may be allowed (at the school's discretion) to take videos and digital images of their children at school events for their own personal use (provided that such videos and images do not potentially infringe data protection legislation). To respect everyone's privacy, and in some cases for safeguarding reasons, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in the digital or video images;
- Staff and volunteers may be authorised to take digital / video images to support educational aims, but must follow school policies and procedures concerning the sharing, distribution and publication of those images. Such images should only be taken using school equipment (personal equipment belonging to staff should not be used for such purposes, except with the explicit permission of a member of the school leadership teaml);
- Care should be taken to ensure that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute, when taking digital / video images;
- Children must not take, use, share, publish or distribute images of others without their permission from the school;
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images, and only where written permission from the relevant parent / carer has been obtained;
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Student's work will only be published with the permission of the student and parent / carer.

16.3 In order to ensure that the internet is used in an appropriate manner, the following controls will be implemented:

- Effective filtering systems will be established to eradicate any potential risks to children through access to, or trying to access, certain websites which are harmful or use inappropriate material;
- Any requests by staff for websites to be added or removed from the filtering list must be approved by the headteacher in advance;
- All school systems will be protected by up-to-date virus software;
- Master users' passwords will be available to the headteacher for regular monitoring of activity;
- At the school's discretion, staff may allowed to use the school internet for personal use during out-of-school hours, as well as break and lunch times so long as such use complies with the school's acceptable use agreement and other relevant school policy;
- Staff and student personal use of the school's internet may be monitored by the digital-safety coordinator where it is deemed justifiable and necessary in order to uphold school policy, for safeguarding purposes and/or to protect children, staff and the school, and where the need for monitoring outweighs the need for privacy.
- Suspected inappropriate internet access by staff will be dealt with in line with the staff discipline policy.

17 Management of the School's Website

17.1 The school's website is an important vehicle for communication with parents/carers and the local community, outside agencies and prospective parents. The Headteacher has overall editorial responsibility, ensuring content is accurate and appropriate, accurate, up-to-date and meets government requirements.

17.2 Personal information relating to staff and children is not published on the website. Images and videos are only posted on the website in accordance with parent/carer wishes, or staff wishes, as appropriate.

17.3 The school website will comply with the school's Publications Scheme including Website, as well as with guidelines for publications including respect for intellectual property rights, privacy policies and copyright. It will include the statutory content required of school websites under law.

18 Communications

18.1 Rapidly developing communication technologies have the potential to enhance learning; such use of communication technologies in school will have regard to the following:

- Users should be aware that school email communications are monitored;
- Staff and children should only use school email in order to conduct school business, using the school email service within school or via the school's remote access provision;
- In line with school policy, users must immediately report 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 children or parents / carers (email, chat, vle etc) must be professional in tone and content. These communications must only take place through official school systems. Staff and child's personal contact details (eg. Email

addresses, phone numbers) or social media accounts must not be used for these communications;
- Whole group school email addresses may be used at ks1, while children at ks2 and above will be provided with individual school email addresses for school use;
- Children should be taught about digital-safety issues, such as the risk of sharing of personal details, images etc. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;

18.2 The school has considered the benefits and risks associated with using technology for educational purposes and, in conclusion, has identified the uses deemed to be acceptable / unacceptable in school, as outlined in Appendix 7 – Communication Technologies Usage Chart.

18.3 The school's Data Protection Policy should be referred to in relation to the recording, processing and transferring of personal data.

19 Tablet Devices

19.1 Tablet devices, such as iPads, have the potential to significantly enhance learning and teaching. When children are using any such school device, staff will ensure that:
- Only age-appropriate, suitable software applications ("apps"), which have been checked in advance, are used;
- Children are frequently reminded of the importance of keeping themselves safe when using the internet, and of strategies to deal with accidental access to inappropriate materials;
- Children are reminded of the behavioural expectations at alma primary when finding, using and sharing information, images, recordings or other activities;
- Children's use of technology is monitored to ensure that they are using technology appropriately to support learning and develop healthy relationships with technology.

20 Social Media - Protecting Professional Identity

20.1 Alma Primary has a duty of care to provide a safe learning environment for children and staff. Expectations for teachers' professional conduct are set out in 'Teachers Standards' (updated 2021). All staff at Alma Primary are expected to behave in an appropriate, professional manner in their uses of technology, including social media. A Staff member who uses social media to harass, cyberbully, discriminate on the grounds of any protected characteristic, or who defame a third party (whether or not the staff member claims to be representing the school) may be in breach of their contract of employment, school policy and/or fall short of the school's reasonable expectations. Any such inappropriate action may result in the staff member being subjected to disciplinary procedures in accordance with school policy.

20.2 The school provides guidance to staff on limiting third party access to personal information so as to minimise the risk of harm to children, staff and the school. Induction training for staff and annual refresher training for all staff will include:
- Guidance on acceptable use; social media risks; checking of settings; data protection; reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

20.3 It is the responsibility of school staff to ensure, in their use of social media, that:

- No reference is made in social media to children, parents / carers, volunteers 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 use of social media for school purposes will be checked regularly by the Digital-Safety Coordinator to ensure compliance with relevant school policies. Staff members must be authorised by the Headteacher to access to the school's social media accounts.

21 School Actions & Sanctions

21.1 It is important that any incident of online services misuse is dealt with as soon as possible and in a proportionate manner, in accordance with the school policy and the school's disciplinary procedures.

22 Managing, Monitoring and Review

22.1 The school recognises that the online world is constantly changing; therefore, the DSL, Digital-Safety Coordinator and the Headteacher will conduct termly light-touch reviews of this policy to evaluate its effectiveness.

22.2 The Governing Body, Headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents that occur. Any changes made to this policy are communicated to all members of the school community as soon as practicable.

Appendix 1: Acceptable Use Agreements for children in Reception and Key Stage 1

Student Acceptable Use Agreement for Younger children

Child's name: Date:

At Alma Primary this is how we stay safe when we use computers:

- I will ask a teacher or school adult if I want to use the computers;
- I will only use activities that a teacher or school adult has told or allowed me to use;
- I will take care of school computers and other equipment;
- I will ask for help from a teacher or school adult if I am not sure what to do or if I think I have done something wrong;
- I will tell a teacher if I see something that upsets me on the screen;
- I know that if I break the rules I might not be allowed to use a computer.

I agree to follow these rules and use school equipment in a safe and sensible way, so that there is no risk to my safety or to the safety of others. I know that my school expects me to behave sensibly at all times and that my teachers will regularly check work I have done on school devices. I understand that these rules are designed to keep me safe and that if I do not follow these rules: I might not be allowed to use school equipment, including ipads. I might not be allowed to do certain activities. My Headteacher and my parents/carers may be told

I confirm that my child and I have discussed the school's digital safety rules and that my child agrees to follow these rules. I agree to support Alma Primary staff if my child does not follow these rules when using devices in school, in relation to other school children and or in relation to school work.	
Parent / Carer Name & Signature	

Appendix 2: Acceptable Use Agreements for children in KS2

I understand that I must follow these rules and use equipment in a safe and sensible way, so that there is no risk to my safety or to the safety of others.

If I do not follow these rules:

- I might not be allowed to use computers, iPads or other equipment in school;
- I might not be allowed to do certain activities;
- My Headteacher and my parents may be told.

Digital-Safety Rules

- I will only use polite and respectful language, making sure that all digital communications with children, teachers or others is responsible and sensible;
- I will always ask permission of those involved before taking or sharing pictures, or video footage;
- Any comments I make will be kind and I will not write anything that might upset someone or give the school a bad name;
- I will treat all equipment and work of others with respect and I will not use school devices in any way that stops other people using them;
- I will tell a teacher if there is problem with a computer;
- I will only access other people's folders with their permission;
- I will not share my username and passwords with anyone except my parents and if I think someone has learned my password then I will tell my teacher;
- I will not use websites to tell anyone my name, where I live, or share my phone number;
- I will change my password regularly and I will never use other people's usernames and passwords or use computers left logged in by them;
- I will ask only use the internet in school when a teacher tells me I can;
- I will only open email attachments from people I know are safe and I will not download or install software on school devices;
- I will use the apps and websites my teachers tells me to use and won't try to use other sites or apps without checking;
- I will always ask for permission from a teacher before using a personal memory stick or digital storage device that I have brought from home;
- I will tell my teacher straight away if any websites that make me feel uncomfortable or if I am sent any messages that make me feel uncomfortable;
- I will not deliberately browse, download, upload or forward material that is illegal or that I know might upset others. If I find something that I think I should not be able to see, I will tell my teacher straight away and I will not show it to other children;
- If someone on the internet asks me to meet them I will tell my teachers or my parents/carers and I will only meet them if my parents/carers or teachers agree;
- I will support the school's approach to online safety and I will take full responsibility for my behaviour when using digital equipment or when using the internet, including responsibility for the resources I access and the language I use;
- I will behave in accordance with this agreement, when using any device that is personal or school property, and whether I am in school or outside of school.

I agree to follow these rules and use school equipment in a safe and sensible way, so that there is no risk to my safety or to the safety of others. I know that my school expects me to behave sensibly at all times and that my teachers will regularly check work I have done on school devices. I understand that these rules are designed to keep me safe and that if I do not follow these rules:

- I might not be allowed to use school equipment, including ipads.
- I might not be allowed to do certain activities.
- My Headteacher and my parents/carers may be told

I confirm that my child and I have discussed the school's digital safety rules and that my child agrees to follow these rules. I agree to support Alma Primary staff if my child does not follow these rules when using devices in school or outside, in relation to other school children and/or in relation to school work, in accordance with the schools Digital Safety Policy and the school's Preventing Bullying Policy.	
Parent / Carer Name & Signature	

Appendix 3: Acceptable Use Agreements for Staff, Governors and Volunteers

Staff, Governor and Volunteer Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for children learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that children receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed digital-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in accordance with the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person, in accordance with school policy.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- I will communicate with others in a professional manner and refrain from using aggressive or inappropriate language. I appreciate that others may have different opinions to my own.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with school policy. I will not use my personal equipment to record these images, unless I have permission to do so from the Headteacher.
- I will only communicate with children and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the establishment:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses wherever reasonably possible.
- I will not open any hyperlinks in emails or any attachments to emails where the source is not known to me or trusted, or where I have any concerns about the validity of the email.
- I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school computer or device, or store programmes on a computer, nor will I try to alter computer settings, without advanced permission from the ICT Digital-Safety Coordinator or Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, I will ensure that it is sent via an encrypted email account.
- Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access will be kept private and confidential, except when I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or fault involving equipment or software, however this may have occurred.

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

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

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

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and, in the event of illegal activities, the involvement of the police.

I have read and understand and agree to the terms set out above and will abide by this agreement.

Staff, Governor or Volunteer Name	
Signed	
Date	

Appendix 4: Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- That community users of school digital technologies will use systems and devices responsibly;
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- That users are protected from potential risk in their use of these systems and devices .

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into Alma Primary.

- I understand that my use of school systems and devices and digital communications may be monitored;
- I will not use a personal device that I have brought into school for any activity that would be inappropriate or illegal in a school setting;
- I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have occurred and I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person, in accordance with school policy.
- I will not publish or share any information I have obtained whilst in the school, on any personal website, social networking site or through any other means, unless I have expressed permission from the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others, including install software on a school device without appropriate permission;

Access to the school's ICT systems or internet is at the sole discretion of the school and may be withdrawn at any time.
I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices.
I understand that the school shall not be liable for any loss of profits and/or for any special, indirect, incidental or consequential loss or damage arising out of or in connection with the school's internet or ICT systems.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in accordance with the above.

Community User Name			
Signed		Date	

Appendix 5: Form for responding to incidents of misuse

Record of reviewing devices and/or internet sites

Individual/Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Reference details for computer used for review (for web sites)

Server ref detail	
Make and model	
IP address	

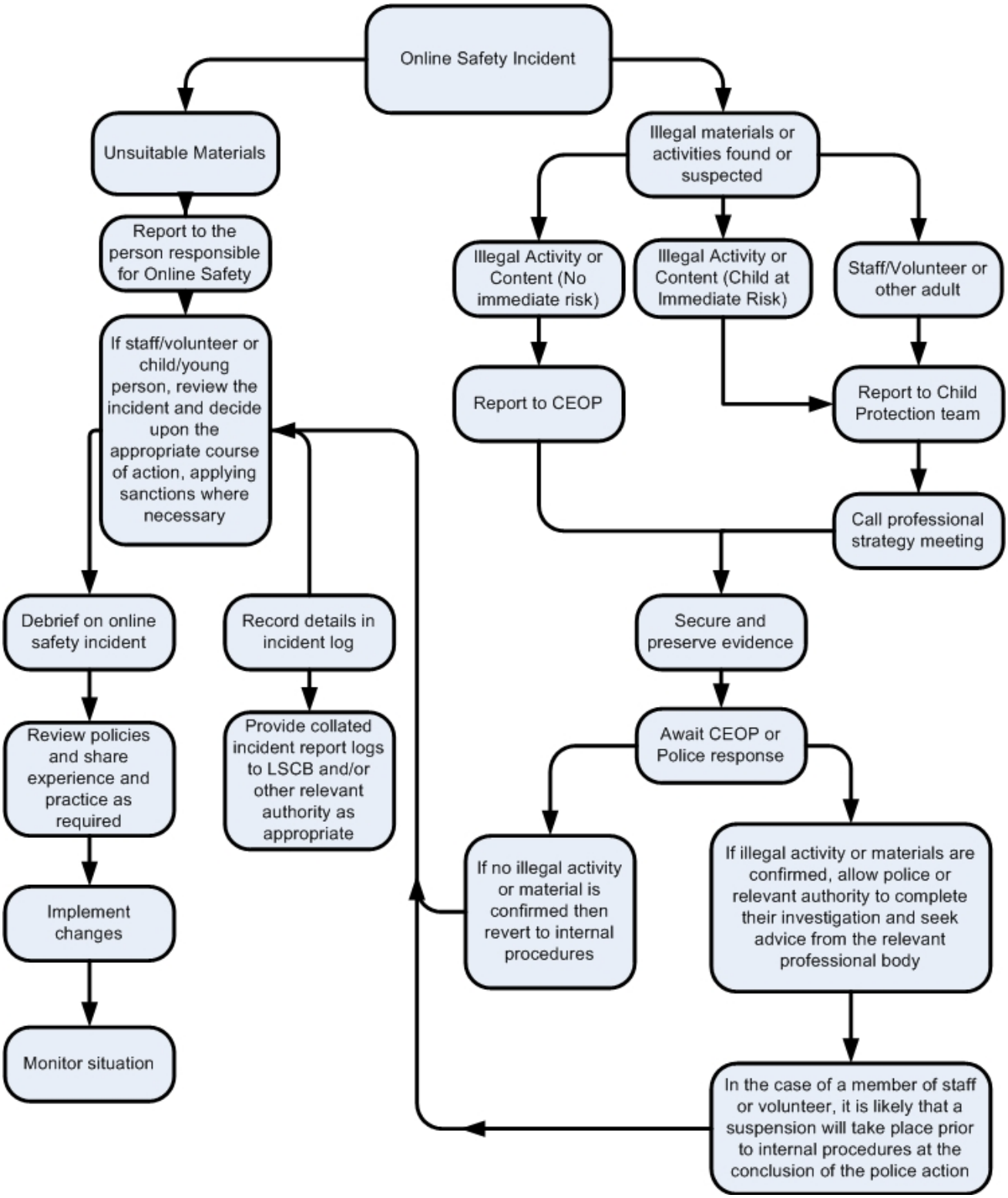
Reason for concern

Web site(s) address / device	Details

Conclusion

Focus	X	Action / Comment
No concern		
Kept on file		
Parents informed		
Referred to Safeguarding board		
Referred to Police		
Other:		

Appendix 6: Online Safety Incident flowchart



Appendix 7: Communication Technologies Usage Chart

Communication Technologies	Staff & other adults				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed as part of a lesson	Allowed with staff permission
Mobile phones may be brought to school		X						X
Use of mobile phones in lessons	X				X			
Use of mobile phones in social time		X			X			
Taking photos on mobile phones / cameras		X						X
Use of other mobile devices e.g. tablets, gaming devices		X					X	
Use of personal email in school / on school network		X					X	
Use of school email for personal emails		X				X		
Use of messaging apps			X		X			
Use of social media		X				X		
Use of blogs		X					X	