Archbishop Cranmer C. of E. Primary Academy

Online Safety Policy

'Striving for Life in All its Fullness'

John 10:10

Reviewed by: Headteacher	October 2022
Updated by : Deputy Head in line with KCSIE Updates 2023	August 2023
Authorised by: Governing Body (if applicable)	Shared: October 2022
Ratified by: Governing Body (if applicable)	October 2022
Date for next review (or earlier should legislation require it)	October 2024

'Striving for life in all its fullness'
John 10[10]

Our Christian Vision

Jesus said *'I have come that they may have life in all its fullness' John 10:10.*
At Archbishop Cranmer C of E Primary Academy we strive for life in all its fullness, for all our children, staff and school community.

Our Mission Statement

- **For Life in all its Fullness for today…**
  - Archbishop Cranmer is a small, caring Church of England Primary School in Aslockton, Nottinghamshire. We are a family community with Christian Values at the heart, where adults and children genuinely care for one another.
  - We **aspire** to be a high achieving school that provides an outstanding education and **culture of opportunity** for all.
  - We believe that every child is unique and valued by God, with their **profound personal development** being at the heart of all we do.
  - We provide a rich and stimulating curriculum that inspires and challenges all to achieve.
  - We foster warm partnerships with parents, the local community, St Thomas's church and local charities.

- **For Life in all its Fullness for the future**…
  - We teach our children to be excellent Christian role models for the future world.
  - We are inclusive, respectful and celebrate global diversity.
  - We provide excellent care, guidance and support to enable our children to keep themselves happy, healthy and safe in their adult lives.
  - We educate children on the importance of their well-being today and in their future.

Our Christian Ethos

Archbishop Cranmer C of E Primary Academy strives to be an inclusive community where children grow, learn and achieve together. Our Take Care Learning Behaviours, held together by our Christian Values, form the essence of our ethos and gives our school its sense of value and drive. We always challenge our school community to consider what our values mean to them.
Our Take Care Hand reminds us that we are always:

- Taking Care (forming meaningful relationships with ourselves and others)
- Aspiring to have a go (being creative and curious)
- Acting with Integrity (always doing the right thing)
- Working hard (aspiring to be the best we can be by embracing high challenge, creative work)
- Being proud of ourselves (growing in confidence, knowing what is possible)

It is our vision is to make the children at Archbishop Cranmer CE Academy as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyber bullying and becoming a positive e-citizen.

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where permitted).

Contents

1. Scope of the Policy

This Online Safety Policy outlines the commitment of Archbishop Cranmer C of E Primary Academy to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy was produced following the legislative framework outlined in Appendix 1.

2. Policy Development, Monitoring and Review

This policy has been developed by the following members of staff:

- Head teacher and Senior Designated Safeguarding Lead
- Deputy head teacher, Designated Safeguarding Lead, Computing and eSafety Lead
- SENCo and Designated Safeguarding Lead.

School will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring of internet activity
- Internal monitoring data for network activity
- Pupil, staff and parent/ carer feedback.

3. Policy and Leadership

3.1 Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and the deputy head teacher have the responsibility to be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by Mrs Sarah Rowe, who will receive regular information about online safety via governor reports provided by the subject leader. The governor with responsibility for Online Safety will have:

- Regular meetings with the Online Safety Lead (Mrs Lauren Rogers);
- Receive reports of online safety incidents
- Check the provision outlined in the policy.

The governing body will also support the school in encouraging parents and carers and the wider community to become engaged in online safety activities.

Online Safety Lead:

The online safety lead will:

- Work closely on a day-to-day basis with the Designated Safeguarding Lead(s) (DSLs), where these roles are not combined
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- Have a leading role in establishing and reviewing the school online safety policies and documents
- Promote an awareness of and commitment to online safety education and raise awareness across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, progressive, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- Provide (or identify sources of) training and advice for staff, governors, parents and carers and pupils
- Liaise with technical staff (RM) and support staff as relevant
- Meet regularly with the online safety governor to discuss current issues, review incidents and, if possible, filtering and monitoring logs
- Attend relevant governor meetings
- Report regularly to the Head teacher and senior leadership team
- Liaise with the local authority and MAT, as required.

<u>Designated Safeguarding Lead(s):</u>

The DfE guidance 'Keeping Children Safe in Education' (2022) states: "*The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description"; Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."*

The Designated Safeguarding Lead(s) should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data (see Data Protection Policy)
- Access to illegal/ inappropriate materials
- Inappropriate online contact with adults/ strangers
- Potential or actual incidents of grooming
- Online bullying.
- recognising the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.child on

<u>Curriculum Leads:</u>

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- iLearn2 Computing scheme of work, supported with Google's Be Internet Legends in Key Stage 2;
- HeartSmart RHE and Christopher Winters RSE schemes of work;
- Assemblies and pastoral programmes across the year;
- Relevant national initiatives and opportunities such as Safer Internet Day and Anti-Bullying Week.

Teaching and Support Staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/ trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood and signed the staff acceptable use agreement
- They immediately report any suspected misuse or problem to Mrs M Stevens, Mrs L Rogers or Mrs E Hodgson for investigation/ action, in line with school safeguarding procedures
- All digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Aspire MAT Virtual Meeting Policy.
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred, and recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School is aware that they have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite.
- They model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network Manager/ Technical Staff

It is the responsibility of the school to ensure that the outside contractor carries out all of the online safety measures that the school's obligations and responsibilities require. The provider should follow and implement the Online Safety Policy and procedures.

At Archbishop Cranmer, our network and services are provided by RM Education. They are responsible to ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Mrs L Rogers (Online Safety Lead and DSL) for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see Appendix 2 - Technical Security Policy).
- Monitoring software/systems are implemented and regularly updated as agreed in school policies.

Learners

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – see standard shown in Appendix 3)
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices available to them in an appropriate way.

At Archbishop Cranmer we take every opportunity to help parents and carers to understand these issues. This will be communicated through:

- Publishing the Online Safety Policy on the school website
- Providing parents and cares with a copy of the acceptable use agreement
- Publishing information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images
- Providing parent and carer information evenings/ sessions (e.g. Parent Forum); eSafety newsletters; up-to-date information and guidance via the school website; sharing information about national and local online safety campaigns and literature.

Parents and carers are encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school
- The use of their children's personal devices in the school.

4. Policy

The Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction
- Is published on the school website.

5. Acceptable Use Agreement

The Online Safety Policy and Acceptable Use Agreement defines acceptable use at Archbishop Cranmer. The acceptable use agreements are communicated and reinforced through:

- Staff handbook
- Our Computing and RHSE curriculum
- Communication with parents and carers
- Our school website
- Policies and standards, such as (but not limited to):
    - Child Protection Policy
    - Child-on-Child Abuse Policy

- Anti-Bullying Standard
- Standard for Mobile Phones and Smart Watches
- Staff Communication Standard
- Visitors to School Standard.

6. Reporting and Responding

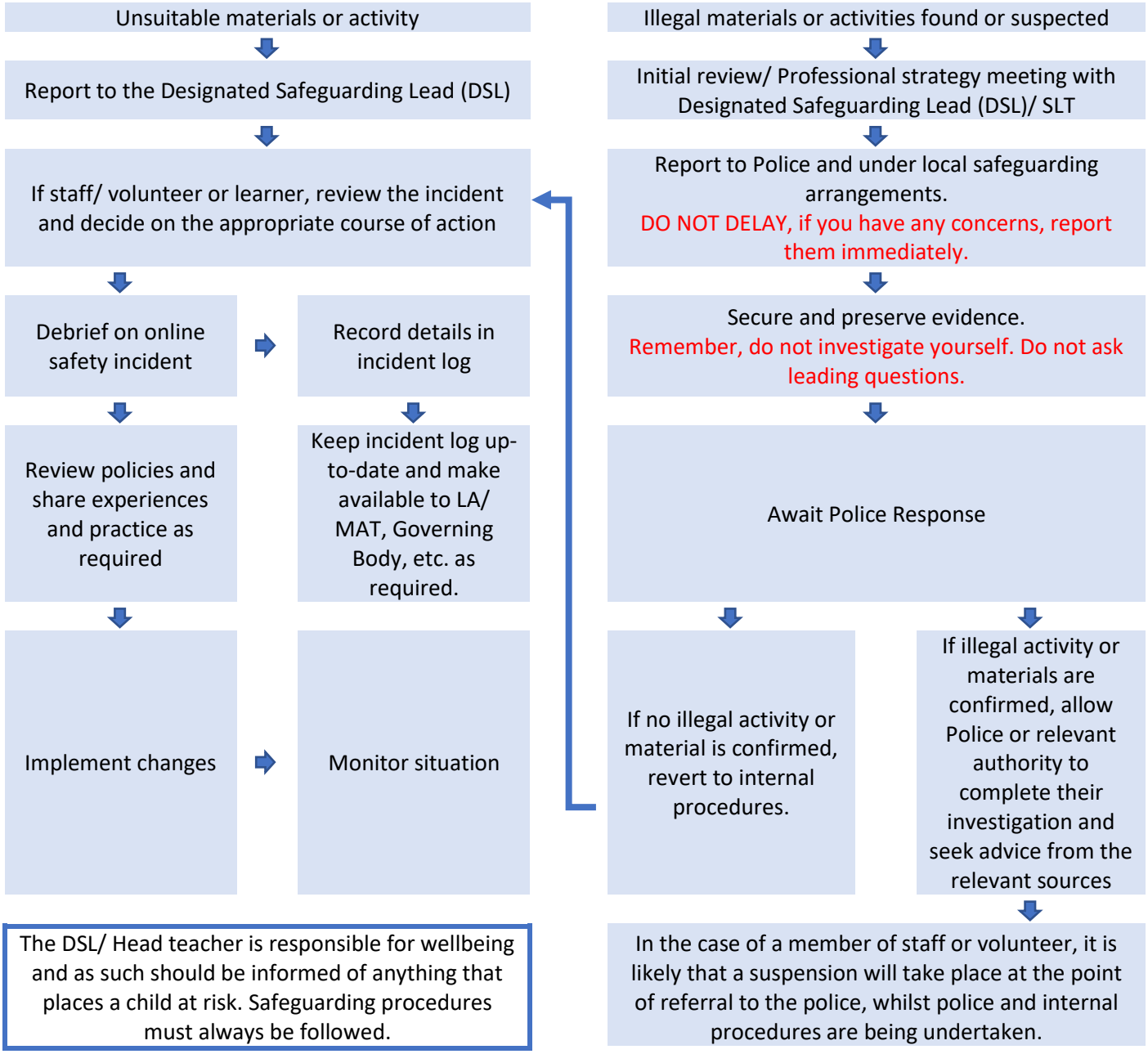
At Archbishop Cranmer, we take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of school (with impact on the school) which will need intervention. We will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, including the whistleblowing, complaints and managing allegations policies
- All members of the school community are made aware of the need to report online safety issues and incidents
- Reports are dealt with as soon as practically possible once they are received
- The DSL(s), Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident is escalated through the agreed safeguarding procedures
- Any concern about staff misuse will be reported to the Head teacher, unless the concern involves the Head teacher, in which case the complaint is referred to the Chair of Governors, LADO or the CEO of the Academy Trust
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action
    - it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
    - there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
    - incidents should be logged using ScholarPack/ CPOMs
    - relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
    - those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
    - learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
        - *the Online Safety Lead and DSLs for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
        - *staff, through regular briefings*
        - *learners, through assemblies/lessons*
        - *parents/carers, through newsletters, school social media, website*

- *governors, through regular safeguarding updates*
- *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*

The below flowchart is available to staff to support the decision-making process for dealing with online safety incidents:

Online Safety Incident Flowchart



It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures, as outlined in our school behaviour policy. In the case of a member of staff or volunteer, the incidents of misuse will be dealt with through the disciplinary procedure policy.

7. Online Safety

At Archbishop Cranmer we recognise that the education of our learners in online safety is an essential part of our online safety provision, we value the implementation of this to help our learners to recognise and avoid risks and develop resilience. Therefore, online safety is a focus across the curriculum where staff reinforce online safety messages.

Our online safety curriculum provides:

- Planned lessons for all year groups from iLearn2, of which are matched against the Education for a Connected World Framework
- Lessons matched to need; these are age-related and build upon prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Assessment opportunities to ensure that pupil learning is progressive and impactful
- Digital competency is planned and effectively through other curriculum areas
- Links to relevant national initiatives and opportunities such as Safer Internet Day and Anti-Bullying Week
- Accessible activities for learners at different ages and abilities
- Reinforcement and safe and responsible adoption of the acceptable use agreement within and outside of school
- Opportunities for staff to role model their use of digital technologies
- Up to date and relevant learning to ensure the quality of learning and outcomes.

8. Staff and Volunteers

All staff will receive online safety training, as recommended within Keeping Children Safe in Education (2022), and understand their responsibilities. The training will be offered as part of annual safeguarding training provided to all staff. All new staff will also receive this as part of their induction programme, ensuring that they fully understand the online safety policy and acceptable use agreements.

The Online Safety Lead and Designated Safeguarding Lead(s) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

This policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.

The Online Safety Lead will provide advice, guidance and training to individuals as required.

9. Technology

At Archbishop Cranmer we are responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

9.1 Filtering

- Filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/ behaviours
- The school manages access to content across its systems for all uses and the filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate Filtering
- Access to online content and services are managed for all users
- Illegal content is filtered by the provider
- There are established routes for users to report inappropriate content.

9.2 Monitoring

At Archbishop Cranmer we have monitoring systems in place to protect the school, systems and users:

- We monitor all network use across all its devices and services
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored

- There are effective protocols in place to report abuse/ misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of this is consistent with the Child Protection Policy.

We follow the UK Safer Internet Centre Appropriate Monitoring guidance and protect users and school users and systems through the use of the appropriate blend of strategies including:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, monitored and reviewed
- Filtering logs are analysed and breaches are reported to senior leaders.

9.3 Technical Security

Our technical systems will be managed to ensure that the school meets the recommended technical requirements of the MAT Data Protection Policy.

- There are regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located
- There are verified back-up routines
- All users have clearly defined access rights to school technical systems and devices
- All users have responsibility of the security of their username and password and must not allow other users to access the systems using their details. Users must immediately report any suspicion or evidence that there has been a breach of security
- The school network and system is protected by secure passwords. RM Education will provide all users with a username and password
- Records of learner usernames and passwords can be kept in an electronic or paper-base form, but they must be kept securely when not required by the user.
- RM Education are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates are applied
- An appropriate system of logging and raising tickets with RM Education support advisers is in place for users to report any potential/ actual technical incident/ security breaches
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The infrastructure and individual workstations are protected by up-to-date endpoint software
- Guests such as trainee teachers, supply teachers and visitors are provided with temporary access to internet software on their own devices which is provided by the school office.

9.4 Mobile Technologies

Our school Acceptable Use Agreement and Standard for the Use of Mobile Phones and Smart Watches outlines the expectations around the use of mobile technologies.

School owned/ provided devices:

- These are allocated to teaching staff only
- Devices are encouraged to be kept on school premises at all times, however these may be taken off site with the permission of the Head teacher
- Staff are encouraged not to use school owned/ provided devices for personal use
- Staff are permitted to install apps/ change settings/ manage devices as required for work-related purposes
- Technical advice should be sought from our support provider RM Education
- Staff are encouraged to use cloud services to save documents and files to allow for flexibility of use across devices
- Should be used in accordance with the Acceptable Use Agreement and Data Protection Policy
- Liability for damages are with the primary user of the device.

10 Social Media

At Archbishop Cranmer we recognise the widespread use of social media for professional and personal purposes and that we have a duty of care not only under the expectations outlined in the DfE Teacher Standards for teachers'

professional conduct, but also to provide a safe learning environment for all. Therefore the following reasonable steps are implemented to minimise risk of harm to learners:

- Ensuring personal information is not published
- Learning links to acceptable use, age restrictions, social media risks, checking settings, data protection and reporting
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Guidance for learners, parents and carers.

School staff should ensure that:

- No reference should be made in social media to learners, parents/ carers or school staff
- They do not engage in online discussion on personal matters relating to 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
- They act as positive role models in their use of social media.

When using official school social media:

- Log in details are shared by senior leaders
- The administration, moderation and monitoring of these accounts are led by senior leadership
- Staff are encouraged to access these sites using school owned devices
- Incidents relating to these accounts may be dealt with under school disciplinary procedures.

Monitoring of public social media:

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

11 Digital and Video Images

At Archbishop Cranmer we recognise that the development of digital images technologies has created significant benefits to learning. However, staff, parents, carers and learners need to be aware of the risks associated with publishing digital images on the internet. We will inform and educate users about these risks and will implement practices to reduce the likelihood of the potential for harm by:

- Using live-streaming or video-conferencing services in line with our MAT policy guidance
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images
- Staff and volunteers are made aware of those learners whose images must not be taken or published
- Images should only be taken on school devices
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents and carers will be obtained before photographs or videos are taken for use in school or published on the school website/ social media

- Parents and carers will be informed of the purposes for the use of images, how they will be stored and for how long in line with the MAT Data Protection Policy
- Images are stored securely in line with the MAT Data Protection Policy.

12 Online Publishing

At Archbishop Cranmer we communicate with parents, carers and the wider community and promote the school through our:

- Public-facing website
- Social media (Facebook and Twitter)
- Online newsletters (shared via email and published to our school website)

The school website is managed/hosted by Primary Site. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

Our public online publishing provides information about online safety through publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, shared via an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process. This is accessible via the CEOP button on our school website.

13 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

For further information relating to the school's practice, please see the MAT Data Protection Policy.

When personal data is stored on any mobile device or removable media the:

- Data will be encrypted, and password protected
- Device will be password protected
- Device will be protected by up-to-date endpoint (anti-virus) software
- Data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- Only use encrypted data storage for personal data
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

14 Impact

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1 – Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

- Computer Misuse Act 1990
- Data Protection Act 1998; 2018
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 159 and 1964
- Human Rights Act 1998
- Education and Inspections Act 2006; 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015
- Criminal Justice and Courts Act 2015

Appendix 2 – Technical Security Standard

Introduction
Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy (see Data Protection Policy)
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities
The management of technical security will be the responsibility of RM Education, which will be monitored in school by Computing and Online Safety Lead Mrs L Rogers.

Technical Security

Policy statements
The school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems, and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level)
- all users will have clearly defined access rights to school technical systems.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- RM Education are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- the school's infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security
A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by RM Education who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Records of learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Training/Awareness:

Members of staff will be made aware of the school password standard:

- at induction
- through the school online safety policy and password security standard
- through the acceptable use agreement

Learners will be made aware of the school's password policy:

- in lessons as part of our Computing and eSafety curriculum
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:
The responsible body (RM Education) will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

Appendix 3 – Standard for Mobile Phones and Smart Watches

Archbishop Cranmer C of E Academy

'Striving for life in all its fullness' John 10:10

Standard for Mobile Phones and Smart Watches

Background

At Archbishop Cranmer CE Primary Academy, the welfare and well-being of our pupils is paramount. The aim of the Mobile Phone and Smart Watch Standard is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones and smart watches are effective communication tools.

This Standard applies to all individuals who have access to personal mobile phones and smart watches on site. This includes staff, volunteers, school stakeholder committee members, children, young people, parents, carers, visitors and contractors. This list is not exhaustive. This standard should also be read in relation to the following documentation:

- Safeguarding Policy
- E-Safety Policy
- Anti-Bullying Policy
- Guidance for photographing and recording children during events and activities
- Code of Conduct Policy
- Staff Handbook

Our aim is therefore that all practitioners:

- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Are responsible for self-moderation of their own behaviours.
- Are aware of the importance of reporting concerns, promptly.

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting, which is agreed to by all users.

Personal Mobiles and Smart Watches

Staff/Volunteers/ Peripatetic teachers/Visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.

- Staff should have their phones on silent or switched off and out of sight (e.g. in a bag, drawer or cupboard) during class time. Smart watches can be worn during school day by staff but the camera, messaging and call services must be disabled.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones (including receiving/sending texts and emails on smart watches and mobile phones) should be limited to noncontact time when no children are present

e.g. in office areas, staff room, empty classrooms.

- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Head teacher aware of this and arrangements will be made with the school office so that the emergency call can be received.
- Staff are not at any time permitted to use recording equipment on their mobile phones/smart watches, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras and iPads.
- Staff should report any usage of mobile devices that causes them concern to the Head teacher.

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication during offsite activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional.
- Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the school office.
- Where parents are accompanying trips they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone/smart watch to take photographs of children.

Personal Mobiles and Smart Watches

We recognise that mobile phones/smart watches are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and could provide a means of bullying or intimidating others. Therefore:

- Pupils are not permitted to have mobile phones at school unless they are in Year 5 or 6 and have been given permission to walk home alone. These phones must be switched off and will be left in the school office upon arrival in school and collected at the end of the day - (the phone is left at the owner's own risk).
- Smart watches should not be brought to school: they may be valuable and could be lost or stolen. Any Smart watches worn by children must not have any internet connection whilst in school.
- Where mobile phones are used in or out of school to bully or intimidate others, then the head teacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site.'

Volunteers, Visitors, School Stakeholder Committee Members, Peripatetic Teachers and Contractors

All volunteers, visitors, committee members and contractors are expected to follow our mobile phone and smart watch policy as it relates to staff whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones/smart watched. It is recognised that a smart watch may be visible on an adult's wrist, but they must be in silent mode and not used during the working day other than to read the time.

While we would prefer parents and carers not to use their mobile phones whilst at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We therefore will ask that parents' and carers' usage of mobile phones, whilst on the school site, is courteous and appropriate to the school environment.

We also allow parents and carers to photograph or video school events such as shows or sports day using their mobile phones/tablets if there are no parental objections or safeguarding issues, – but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own.