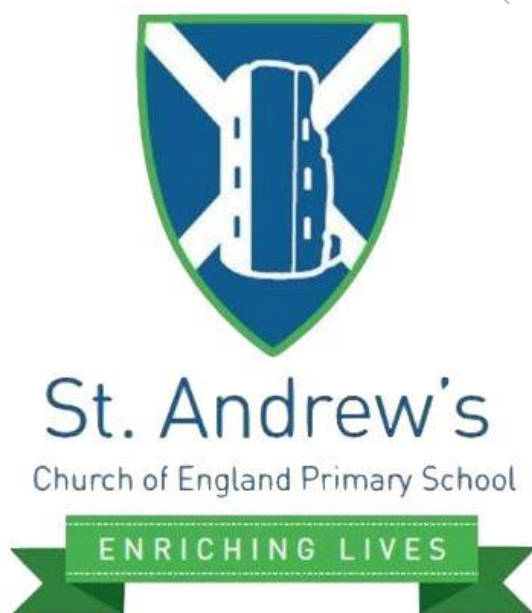




Online Safety Policy

Spring 2023

(This policy has been adapted from the SWGfL School Online Safety Policy Templates.)

We believe that every person in our school community should flourish and broaden their horizons. Therefore, it is the element of 'enrichment' that defines our school; we are a church school that endeavours to provide the widest of opportunities for all.

Within our caring and nurturing environment and guided by our shared Christian values, we aim to ensure that all voices in our school family can be heard and all are engaged in learning that develops and challenges them, excites their imagination and provides an opportunity to achieve their full potential.

We see everyone and everything as valued in the eyes of God and recognise that all the members of our family are individuals as we work together towards a society of mutual respect, compassion and justice.

Even the smallest person can change the course of the future." JRR Tolkien

1. Scope of the Policy

- 1.1 This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school .
- 1.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils 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 cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school , but is linked to membership of the school. 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 published Behaviour Policy.
- 1.3 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

2.1 Governors:

- 2.1.1 Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

2.2 Headteacher / SLT ensure:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety

allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures). (see procedures – p29/30)

- The Headteacher / Senior Leaders are responsible for ensuring that the Headteacher and other relevant staff receive suitable training to enable them to carry out their online safety roles and to 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (see APPENDICES)
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs (see APPENDICES)
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

2.3 Headteacher / Technical staff ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Group / other relevant body Online Safety Policy / guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that 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
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher
- that monitoring software / systems are implemented and updated as agreed in school policies

2.4 Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) (*see APPENDICES*)
- they report any suspected misuse or problem to the Headteacher (*see APPENDICES*)
- all digital communications with students / pupils / 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
- students / pupils understand and follow the Online Safety Policy and acceptable use policies (*see APPENDICES*)
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices (*see APPENDICES*)
- in lessons where internet use is pre-planned students / pupils 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

2.5 Designated Safeguarding Lead

2.5.1 Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

2.6 Online Safety SLT/MLT Group

2.6.1 The Online Safety Group provides a consultative group that can draw on wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body .

2.6.2 Members of the Online Safety Group will assist the Headteacher with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes (*see APPENDICES*)
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs (*see APPENDICES*)
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of self-review

2.7 Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement (*see APPENDICES*)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying (*see APPENDICES*)
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 's Online Safety Policy covers their actions out of school, if related to their membership of the school

2.8 Parents / Carers

2.8.1 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

2.8.2 The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events (*see APPENDICES*)
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

2.9 Community Users

2.9.1 Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (*see APPENDICES*)

3. Education – Students / Pupils

3.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in online safety is therefore an essential part of the school's online safety

provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school (*see APPENDICES*)
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / pupils 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the

filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. (see APPENDICES)

4. Education – Parents / Carers

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

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

5. Education – The Wider Community

5.1 The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience.

5.2 This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety Education & Training – Staff / Volunteers

6. Education - Staff

6.1 It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly (*see log – p35*)
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Headteacher(or other nominated person) will receive regular updates through attendance at external training and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Headteacher(or other nominated person) will provide advice / guidance / training to individuals as required.

7. Education – Governors

7.1 Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding.

7.2 This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents

8. Guidance for Staff

8.1 The school recognizes that staff may have access to personal computers at home in addition to school equipment. However, staff are expected to follow a personal code of conduct whenever using any computer. *(see APPENDICES)*

8.2. Internet access

8.2.1 You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

8.2.2 It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Headteacher so that it can be logged. *(see APPENDICES)*

8.2.3 Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK. *(see APPENDICES)*

8.3 Social networking - will be blocked in this school. Where staff use this facility for personal use, they should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available to children at the school. *(see APPENDICES)*

8.4 Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.

8.5 Use of Email - All members of staff should use their professional email address for conducting school business.

8.6 Passwords - Staff should keep passwords private. Passwords are confidential and individual to each person. On no account should a member of staff allow a student to use a staff login. *(see APPENDICES)*

8.7 Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced. *(see APPENDICES)*

8.8 File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted

on the Lincolnshire School's Network.

- 8.9 Personal Use - Staff are only permitted to use ICT equipment for personal use with the express permission of the Headteacher.
- 8.10 Images and Videos – Staff should not store personal images or videos on school equipment as this can significantly impact on the efficiency of the computer network (single images used as desktops or screen savers is permissible). Staff and pupils should not upload onto any internet site images or videos of other staff or pupils without consent. (*see policy – p64*)
- 8.11 Photos should only be taken of children during normal School activities. Cameras should never be taken into the toilets/changing areas. A child should never be photographed when they are changing or in EYFS when nappies are being changed.
- 8.12 Only members of staff who have an enhanced DBS disclosure are permitted to take photographs.
- 8.13 Photographs taken by members of staff on their own cameras can only be downloaded onto a school lap-top/computer. No images are to be downloaded and kept on private lap-tops/computers. No images should be retained on mobile phones and all images must be deleted prior to the member of staff leaving the school premises.
- 8.14 Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. Any such use should be stringently checked for up to date anti-virus and malware checkers.
- 8.15 Viruses and other malware - any virus outbreaks are to be reported to the Headteacher as soon as it is practical to do so, along with the name of the virus (if known).

9. Technical – infrastructure / equipment, filtering and monitoring

- 9.1 The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. (*see APPENDICES*)
- 9.2 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
- All users will have clearly defined access rights to school technical systems and devices.
- All adult users will be provided with individual username and secure password by the Headteacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every.
- The “master / administrator” passwords for the school ICT system, is known by the Headteacher and the IT Support Teacher
- Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing Netsweeper and the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.** Additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Users can report any actual / potential technical incident / security breach to the Headteacher
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- The headteacher can provide temporary access for “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Family members are not allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to forbids staff from downloading executable files and installing programmes on school devices without permission.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.** (see appendix - School Personal Data Policy Template in the appendix for further detail)

10. Mobile Technologies (including BYOD/BYOT)

10.1 Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet.

10.2 Use of such equipment can only be made by prior agreement with the Headteacher.

	School owned for single user	School owned for multiple users	Authorised device ¹	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes		
Internet only					
No network access				No	No

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

11. School Web Site

11.1 The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well presented and that personal security is not compromised. An editorial team ensure common values and quality control. Towards this outcome the site content is currently managed by the Headteacher.

11.2 As the school's Web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupils' full names will not be used anywhere on the Web site.
- No names will be used with photographs.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

12. Use of digital and video images

12.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. (*see APPENDICES*)

12.2 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

13. Data Protection

13.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

13.2 A School Personal Data template is available in the appendices to this document.

(see Personal Data Handling Policy – see APPENDICES)

(see Freedom of Information Policy – see APPENDICES)

(see Data Protection Policy – see APPENDICES)

13.4 The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the relevant policy.
- It has a Data Handling and Protection Policy *(see APPENDICES)*
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data

- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

13.5 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

13.6 When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The Personal Data Handling Policy in the appendix provides more detailed guidance on the school's responsibilities and on good practice.

14. Communications

14.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages.

14.2 Children are not allowed to bring into school any mobile device, camera or phone unless it is left in the care of the Classteacher during the course of the day.

14.3 For all other adults the following matrix should be used:

	<i>Staff and other Adults</i>			
	<i>Allowed</i>	<i>Allowed at certain times</i>	<i>Allowed for selected staff</i>	<i>Not Allowed</i>
Communication Technologies				
<i>Mobile phones may be brought to the school/academy</i>	X			
<i>Use of mobile phones in lessons</i>				X
<i>Use of mobile phones in social time</i>		X		
<i>Taking photos on mobile phones/cameras</i>				X
<i>Use of other mobile devices e.g. tablets, gaming devices</i>		X		
<i>Use of personal email addresses in school/academy, or on school/academy network</i>				X
<i>Use of school/academy email for personal emails</i>				X
<i>Use of messaging apps</i>		X		
<i>Use of social media</i>		X		
<i>Use of blogs</i>		X		

14.4 When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Communication between staff and pupils is not permitted.
- Whole class / group email addresses may be used at EYFS, KS1 and KS2.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

15. Social Media - Protecting Professional Identity

15.1 All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority group liable to the injured party. Reasonable steps to prevent predictable harm must be in place. (*see Policy – p60*)

15.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: 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

15.3 School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

15.4 When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

15.5 Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

15.6 Monitoring of Public Social Media

15.6.1 As part of active social media engagement, it is considered good practice to 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

15.6.2 The school's use of social media for professional purposes will be checked regularly by the Headteacher and SLT to ensure compliance with the school policies.

16. Unsuitable / inappropriate activities

16.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

16.2 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Activities that might be classed as cyber-crime under the Computer Misuse Act:					
	- Gaining unauthorised access to school networks, data and files, through the use of computers/devices - Creating or propagating computer viruses or other harmful files - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) - Disable/Impair/Disrupt network functionality through the use of computers/devices - Using penetration testing equipment (without relevant permission)					X
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
	Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Using school systems to run a private business				X	
	Infringing copyright				X	
	On-line gaming (educational)				X	

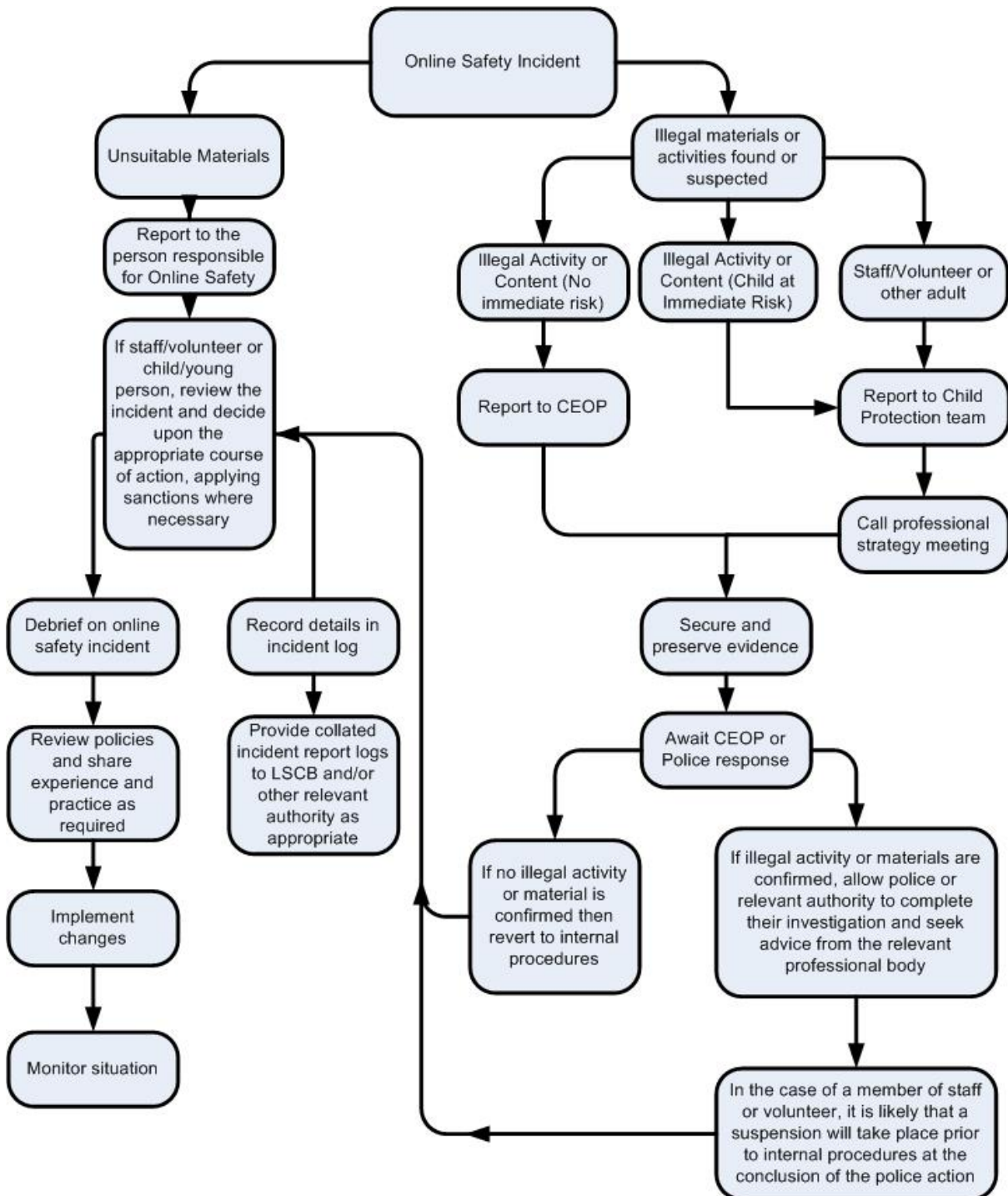
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube/Vimeo			X		

17. Responding to incidents of misuse

- 17.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). *(see logs – p32/33)*

17.2 Illegal Incidents

17.2.1 If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



17.3 Other Incidents

17.3.1 It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. (*see APPENDICES*)

17.3.2 In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority Group or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour

- the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

17.3.4 It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

17.4 School Actions & Sanctions

17.4.1 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 / disciplinary procedures as follows.

17.4.2 Any incident involving a child will be dealt with by the classteacher in the first instance. The classteacher may discuss the matter with the Headteacher prior to taking any action if they are unsure as to how best to proceed.

17.4.3 Any matter involving staff must be referred to the Headteacher and be dealt with under the Staff Code of Conduct Policy. In certain instances, the Headteacher may take professional advice before agreeing a course of action and/or may involve the police.

Appendices

Acceptable Use Policy Agreement – Staff	27
Acceptable Use Policy Agreement – KS2	29
Acceptable Use Policy Agreement – EYFS/KS1	30
Acceptable Use Policy Agreement – Community	31
Responding to incidents of misuse – flow chart	33
Record of reviewing devices / internet sites (responding to incidents of misuse)	34
Reporting Log	35
Change Request Log	36
Training Needs Audit Log	37
School Technical Security Policy (including filtering and passwords)	38
School Personal Data Handling Policy	44
Privacy Notice for Staff	50
Privacy Notice for children	55
Privacy Notice for Parents/Carers	56
Privacy Notice for Governors	61
Freedom of Information Policy	65
School Policy : Electronic Devices - Searching & Deletion	67
Social Media Policy	72
Photographs in School Policy	78

Acceptable Use of ICT Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read and this summary and have an awareness that it forms a part of the school's wider IT Safety Policy (which is available on the school's network). You must sign this declaration to confirm you have read and understood its contents.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business, or personal email addresses for school business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. All school emails should only be accessed on a secure device and phone. Where staff use a personal device this must be passworded and for their sole use and not accessible by a third party.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, teachers may use their staff laptop and ensure that all files are stored in the ‘H drive’. Alternatively, information may be stored in ‘OneDrive’ to be accessible at home. Access to the ‘One Drive’ on a personal computer should not be left open when logging off, nor should it be set to synchronise. Any work should always be removed promptly on returning to school. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out.

Viruses and other malware - any virus outbreaks are to be reported to the Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE :

DATE :

Acceptable Use Policy – KS2 children

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I promise – not to look for or show other people things that may be upsetting.

I promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Child) :

Signed (Parent) :

Date :

Acceptable Use Policy – EYFS & KS1 children

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult 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 / tablet

Signed (child):

Signed (parent):.....

Date:

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- 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 the school :

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- 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 permission from the school.
- I will not, without permission, 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 device, nor will I try to alter computer settings, unless I have permission to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

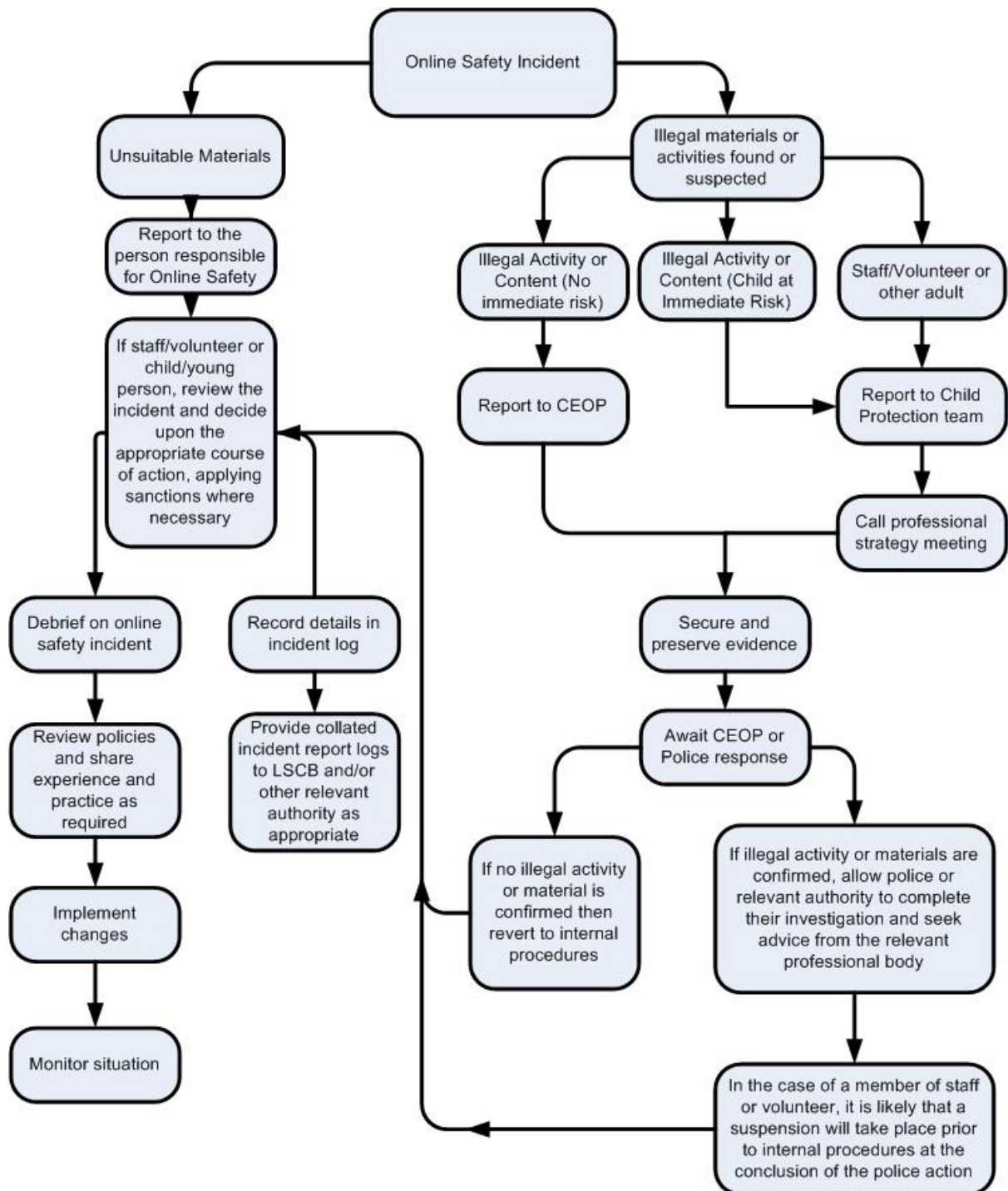
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:

Signed:

Date:

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

.....

.....

.....

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

Name and location of computer used for review (for web sites)

.....

.....

<i>Web site(s) address / device</i>	<i>Reason for concern</i>

Conclusion and Action proposed or taken

Audit Log

Reporting Log						
Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Audit Log

Change Request Log			
Change Request	By Whom	Approved	Date of Change

Audit Log

Training Needs Audit Log				
Group:				
Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

School Technical Security Policy (including filtering and passwords)

1. Introduction

1.1 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
- 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.

2. Responsibilities

2.1 The management of technical security will be the responsibility of the Headteacher.

3. Policy statements

3.1 The school will be 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. 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.

- 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.
- The Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Mobile device security and management procedures are in place.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- A system is in place for users to report any actual / potential technical incident to the Headteacher
- A system is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- Staff are not authorised to give family members access to school devices out of school.
- Staff may use removable media (eg memory sticks / CDs / DVDs) with their own designated devices but must not use such devices on school based machines without permission from the Headteacher.
- The school 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.

4. Password Security

4.1 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 Virtual Learning Environment (VLE).

4.2 All users will 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).

4.3 All school networks and systems will be protected by secure passwords that are regularly changed

4.4 The “master / administrator” passwords for the school systems, is available to the *Headteacher*.

4.5 All users (adults and young people) will 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.

4.6 Passwords for new users, and replacement passwords for existing users will be allocated by the Headteacher.

4.7 Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.

4.8 Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

5. Student / Pupil Passwords

5.1 All users will be provided with a class username and password by the Headteacher.

5.2 Students / pupils will be taught the importance of password security

6. Training / Awareness

6.1 Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

6.2 Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

6. Audit / Monitoring / Reporting / Review

6.1 The Headteacher will ensure that full records (manual or automated) are kept of Security incidents related to this policy

7. Filtering

7.1 The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

7.2 The responsibility for the management of the school's filtering policy will be held by the Headteacher. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

7.3 To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs

7.4 All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

7.5 Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school.

7.6 Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Ark ICT
- The school has provided enhanced / differentiated user-level filtering through the use of a filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)

- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
- *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*

7.7 Education / Training / Awareness

7.7.1 *Pupils / students* will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

7.7.2 Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

7.7.3 Parents will be informed of the school's filtering policy through the Acceptable Use Agreement, the school web site and through newsletter etc.

7.8 Changes to the Filtering System

7.8.1 Levels of filtering are managed by the Headteacher and may be modified by request and subject to formal approval by the SLT. Any changes will be dated and recorded.

7.8.2 Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher will decide whether to make school level changes (as above).

7.9 Monitoring

7.9.1 No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable

School Personal Data Handling Policy

1. Introduction

1.1 Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

1.2 It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

1.3 Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

1.4 Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

2. Policy Statements

2.1 The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

2.2 All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

3. Personal Data

3.1 The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

4. Responsibilities

4.1 Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

4.2 Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5. Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

6. Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset

7. Risk Assessments

7.1 An Information risk audit has been carried out to establish the security measures already in place and whether they are the most appropriate and cost effective.

7.2 Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

9. Secure Storage of and access to data

9.1 The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

9.2 All users will use strong passwords which must be changed regularly. User passwords for adults must never be shared.

9.3 Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

9.4 All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

9.5 Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

9.6 Data should not be stored on any portable computer system not belonging to the school, USB stick or any other removable media:

9.7 The *school* has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

9.8 The *school* has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

9.9 As a Data Controller, the *academy* is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

9.10 All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

9.11 The *school* recognises that under Section 7 of the DPA,

<http://www.legislation.gov.uk/ukpga/1998/29/section/7>

data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

9.12 The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

10. Disposal of data

10.1 The school will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

10.2 *A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

11. Disposal of Equipment

11.1 Prior to the transfer or disposal of any ICT equipment the System Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

11.2. The Data Protection Act requires that any personal data held on such a machine be destroyed. It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

12. Repair of Equipment

12.1 If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible.

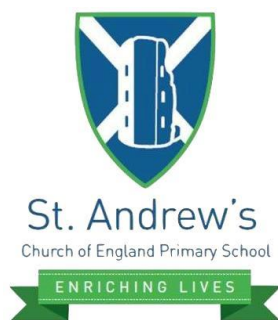
12.2 The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

13. Audit Logging / Reporting / Incident Handling

13.1 The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a “responsible person” for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

13.2 All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.



Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, St Andrew's CE Primary School, Woodhall Spa, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Joe Lee (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of identification documents
- Photographs

- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds, which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule. Our record retention schedule sets out how long we keep information about staff (a copy is available from school or available online at <https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>)

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please do so in writing to Mr. John Whalley, Headteacher in the first instance.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mr John Whalley, Headteacher, in the first instance.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

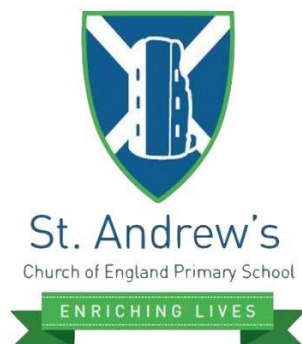
Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

- Joe Lee: dpo@ark.me.uk

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

<https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices>



Privacy Notice for Pupils

When you are at school, the adults need to have, and sometimes keep, information about you.

This will be information such as:

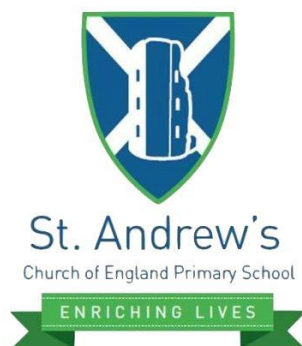
- Your name
- Your birthday
- Where and who you live with
- How often you come to school
- How well you are doing in your work at school
- Photographs or videos of you for use in school, in our Newsletters, on the website or in local media
- Your family beliefs and celebrations
- Any special medicines you need to take or if you see a doctor regularly.

Don't worry, the person you live with will provide this information and they can tell you all about it if you have questions.

Sometimes you tell an adult about something that has upset or worried you. In order to keep you safe and look after you, adults in school may share this information with other adults whose job it is to help children.

We only share information with safe adults and the information cannot be seen without the Headteacher's permission.

If you want to talk to anyone about your information then ask either the adults you live with or the adults in school.



Privacy Notice for Parents/Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, St Andrew's Church of England Primary School, Woodhall Spa, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Joe Lee (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion and behaviour information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds, which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention schedule sets out how long we keep information about pupils (a copy is available from school or available online at <https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>)

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Schools that the pupils attend after leaving our school
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Ofsted and the Lincoln Diocesan Board of Education
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data. <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

You can also contact the Department for Education with any further questions about the NPD.
<https://www.gov.uk/contact-dfe>

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it;
- Tell you why we are holding and processing it, and how long we will keep it for;
- Explain where we got it from, if not from you or your child;
- Tell you who it has been, or will be, shared with;
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this;
- Give you a copy of the information in an intelligible form.

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request for your personal information, or be given access to your child's educational record, please make your request in writing to Mr John Whalley, Headteacher in the first instance.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

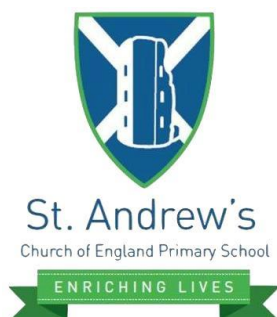
Complaints

Alternatively, you can make a complaint to the Information Commissioner's Office:

- ## Contact us

- Joe Lee: dpo@ark.me.uk

<https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices>



Privacy Notice for Governors and Volunteers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, St Andrew's CE Primary School, Woodhall Spa, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Joe Lee (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Copy of identification documents
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Inform our recruitment and retention policies
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector

- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds, which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain a file for each Governor/volunteer. The information contained in this file is kept secure and is only used for purposes directly relevant to your work at the school.

Once your office as Governor/volunteer period with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule. Our record retention schedule sets out how long we keep information about staff, governors and volunteers (a copy is available from school or available online at

<https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education

- Your family or representatives
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for.
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please do so in writing to Mr John Whalley, Headteacher in the first instance.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mr John Whalley, Headteacher, in the first instance.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

- Joe Lee: dpo@ark.me.uk

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

<https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices>

Freedom of Information Act

1.1 This is St. Andrew's C.E. Primary School Publication Scheme on information available under the Freedom of Information Act 2000

1.2 The governing body is responsible for maintenance of this scheme.

3. Introduction: what a publication scheme is and why it has been developed

3.1 One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

3.2 To do this we must produce a publication scheme, setting out:

- The classes of information which we publish or intend to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment.

3.3 The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is [either available for you on our website to download and print off or] available in paper form.

3.4 Some information which we hold may not be made public, for example personal information.

3.5 This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

4. Aims and Objectives

4.1 The school aims to:

- enable every child to fulfill their learning potential, with education that meets the needs of each child,
- help every child develop the skills, knowledge and personal qualities needed for life and work, and this publication scheme is a means of showing how we are pursuing these aims.

5. Categories of information published

5.1 The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 6 of this scheme.

5.2 The classes of information that we undertake to make available are organised into four broad topic areas:

1. *School Prospectus - information published in the school prospectus.*
2. *Governors' Documents - information published in the Governors Annual Report and in other governing body documents.*
3. *Pupils & policies - information about policies that relate to pupils and the school policies.*
4. *School Policies and other information related to the school - information about policies that relate to the school in general.*

6. How to request information

6.1 If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email, fax or letter. Contact details are set out below or you can visit our website at www.standrews-woodhallspa.org.uk

Email: enquiries@st-andrews-woodhall.lincs.sch.uk
Tel: (01526) 352705

Contact Address:

St. Andrew's C.E. Primary School
King Edward Crescent
Woodhall Spa
LN10 6RD

6.2 To help us process your request quickly, please clearly mark any correspondence "PUBLICATION SCHEME REQUEST" (in CAPITALS please)

School Policy: Electronic Devices - Searching & Deletion

1. Introduction

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

3. Responsibilities

The *Headteacher* is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval.

The Headteacher/Principal will need to authorise those staff who are allowed to carry out searches.

The *Headteacher* has authorised the SLT and MLT to carry out searches for and of electronic devices and the deletion of data / files on those devices.

The *Headteacher* may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

4. Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role. Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

5. Policy Statements

5.1 Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

If pupils / students breach these rules, the sanctions for breaking these rules will be the confiscation of the phone and a subsequent return at home time with the reminder that phones are not allowed in school.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

5.2 In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *student / pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the *student / pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student / pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *student / pupil* of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

5.3 Extent of the search:

The person conducting the search may not require the *student / pupil* to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the *student / pupil* has or appears to have control – this includes desks, lockers and bags.

A *student's / pupil's* possessions can only be searched in the presence of the *student / pupil* and another member of staff, except where there is a risk that serious harm will be caused to

a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

5.4 Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so, however the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

6. Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so, however, the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. In such cases the Headteacher or in his absence a member of the SLT must be contacted.

A record should be kept of the reasons for the deletion of data / files.

7. Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

8. Audit / Monitoring / Reporting / Review

The Headteacher will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Online Safety Committee / Online Safety Governor) at regular intervals.

This policy will be reviewed by the Head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

DfE guidance can be found at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

Social Media Policy

1.1 Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

1.2 *The school* recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

2. Scope

2.1 This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

2.2 This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

2.3 The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

2.4 Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

2.5 Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

2.6 Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

2.7 Digital communications with pupils/students are also considered. Staff may only use on line media to communicate with learners via the school website or Office 365 for remote learning.

2.8 The school maintains its own social media account which is managed by the school. No other accounts are recognised or approved. This is managed by a member of the SLT.

3. Responsibility

3.1 SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

3.2 Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Adding an appropriate disclaimer to personal accounts when naming the school

4. Monitoring

4.1 The school account must be updated regularly.

4.2 However, it is locked down and will not accept comments or replies from third parties.

5. Behaviour

5.1 The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

5.2 Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff.

5.3 The school social media account must not be used for personal gain.

5.4 Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

5.5 Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

5.6 If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.

5.7 Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

5.8 The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

5.9 The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

6. Legal considerations

6.1 Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

6.2 Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

7. Handling abuse

7.1 When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.

7.2 If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.

7.3 If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

8. Tone

8.1 The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards.

8.2 Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

9. Use of images

9.1 School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

9.2 Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.

9.3 Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts

9.4 Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

9.5 If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

10. Personal use – staff

10.1 Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

10.2 Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

10.3 Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

11. Pupil/Students

11.1 Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.

11.2 The school's education programme should enable the pupils/students to be safe and responsible users of social media.

11.3 Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

12. Parents/Carers

12.1 Parents/Carers are encouraged to comment or post appropriately about the school.

12.2 In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

13. Monitoring posts about the school

13.1 As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

13.2 The school should effectively respond to social media comments made by others according to a defined policy or process.

14. Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

15. Managing school social media accounts

15.1 The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

15.2 The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Photographs in School Policy

1.1 The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

1.2 St Andrew's Church of England Primary School welcomes positive publicity. Children's photographs add colour, life and interest to articles promoting school activities and initiatives.

1.3 Making use of photographs for the school in publicity materials can increase pupil motivation and staff morale and help parents and the local community identify and celebrate the school's achievement.

1.4 The Governors and staff of the school recognise that photographs have to be used in a responsible way. We respect the children's and parents' rights of privacy and we are very aware of potential child protection issues.

1.5 The aim of the school's policy is to minimise the risks in relation to the use of photographs in school publicity materials, on its website and in newspapers. To this end all parents will receive a copy of the policy and parental consent will be secured for the use of photographs.

2. Data Protection Act

2.1 Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images for publicity purposes will require the consent of either the individual concerned or in the case of pupils, their legal guardians.

2.2 This means that without consent images of pupils or staff on websites, in publications or in a public place may not be displayed. The definition of a public place includes areas where visitors to the school have access.

3. Implementation

3.1 The implementation of the policy is the responsibility of the whole staff.

4 Pupil images in School Publicity Material

4.1 The following principles will be followed:

- If a child is named, no photograph will be used.

- If an individual photograph is used, no name will be given.
- Only images of children suitably dressed will be used. In activities such as dance and gymnastics the content of the photograph will focus on the activity, not on a particular child.
- No image of a child who is subject to a court order will be used.
- Images will be stored securely and used only by those authorised to do so.

5. Websites

- Consent will be obtained individually for such cases.
- Care will be taken to ensure that a file name of a photograph cannot identify a pupil.

6. Newspapers

- For all photographs names will only be supplied if prior permission has been obtained on the consent from.

(Please note that some newspapers will refuse to publish photographs without a name and as such children may need to be omitted in such cases (if permission is not given).

7. Filming Events

- Registration will be required from every parent/carer wishing to use photographic equipment for personal use at concerts church services, sports days etc., prior to the event. In such cases, parents are only given permission to photograph their own child. ***It is recognised that other children may be included incidentally in these photographs and therefore parents/carers must be aware that they are not being given permission to include these children in any social media uploads and as such may be acting illegally.***
- Parents supporting a school trip or visit are not expected to take photographs of any children (including their own) whilst in a supervisory role.
- All visitors will be expected to turn off camera phones on entering the school.
- Parents or any other spectator will be required to inform the school if they wish to use photographic equipment.
- In certain circumstances a designated area for filming may be identified.

8. Commercial Photography

8.1 If a commercial photographer is used:

- a clear brief on appropriate content and behaviour will be provided
- identification will be worn at all times

- parents will be informed that a photographer will be in attendance
- there will be no unsupervised access to children or one-to-one sessions
- no photo sessions will be allowed outside the event

9. School archive

The school now maintains an archive of photographs on the school network. These photographs are not for general circulation but may form part of future displays or exhibitions. These may be viewed by parents on request and copies may be requested at a nominal charge.