**Be courageous, be strong;**
**Do everything in love.**
**1 Corinthians 16:13-14**

# E-Safety Policy

*The fruit of the Spirit is love, joy, peace, patience, kindness, goodness, faithfulness, gentleness and self-control.* Galatians 5:22

**Intent**

Technology's potential within education is remarkable and we, as a school, aim to not only utilise the wide range of available electronic resources out there where appropriate but also to prepare our children for their future within such a technologically advanced world. Given the ubiquity of such technology, it is our responsibility as a school to, first and foremost, protect children as well as possible. We must deliver an effective approach to online safety which empowers us to protect and educate the whole school community. We must have robust processes in place to ensure the online safety of not only pupils but also staff, volunteers and governors as necessary. Lastly, we must establish clear mechanisms to identify, intervene and escalate an incident where appropriate. This is done according to the school's Christian vision which encourage children to not only marvel in all of God's creation, including technological, but also to 'do everything in love'.

**Schedule for Development/Monitoring/Review**

| | |
|---|---|
| This e-safety policy was approved by the governing body on: | Summer 2022 |
| This implementation will be monitored by: | Headteacher<br>Designated Safeguarding Leads<br>Head of Computing<br>Governors' Teaching, Learning and Assessment (TLA) |
| The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (including anonymous details of e-safety incidents) | Annually, through the TLA committee |
| The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | Autumn full Governing Body meeting. |
| Should a serious e-safety incident take place, the following external persons/agencies may be informed: | Clennell Safeguarding Team<br>GEM Education – School's Computing Support<br>LA Safeguarding Officer<br>Police |

The school will monitor the impact of the policy using:

- Logs of reported incidents using CPOMS
- Monitoring logs of internet activity by the Local Authority IT Support
- Surveys/questionnaires of
    - Children
    - Parents/carers
    - Staff

**Scope of the policy**

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 e-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.

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 e-safety behaviour that take place out of school.

**Roles and Responsibilities**

The school recognise that everyone, from children, to families, to staff, have responsibilities in ensuring pupils are safe online.

*Governors:*

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by Governors' Teaching, Learning and Assessment subcommittee receiving information about e-safety incidents.

*Senior Leadership Team*

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- Under the Regulation of Investigatory Powers Act 2000 (RIPA), the Headteacher can exercise their right to monitor the use of the school's information systems and internet access where she believes unauthorised use may be taking place; to ensure compliance with regulatory practices; to ensure standards of service are maintained; to prevent or detect crime; to protect the communication system and to pick up messages when someone is away from school. If any such monitoring detects the unauthorised use of social networking sites disciplinary action will be taken. For further information, please see the Acceptable Use Policy.
- The Senior Leadership Team (Headteacher, Deputy Headteacher, School Business Manager and other relevant leaders, including the Early Years Leader and other designated safeguarding leaders), and the Computing Lead, share responsibilities as Online Safety Leads. They will deal with all serious e-safety incidents at the direction of the Headteacher as well as being made aware of all relevant incidents by staff and, where relevant, by families.
- The School Business Manager has particular responsibility for liaison (as Network Manager) with Newcastle City Council IT Services who manage the IT service within school. This includes ensuring the filtering protocols are applied and that breaches and attempted breaches of IT services are logged.

*Online Safety Leads (SLT and the Computing Lead)*

As per the Behaviour Policy and the legal powers given to Headteachers (see 'Scope of the Policy', above), Online Safety Leads will deal with any disciplinary procedures for children whose online actions which could bring the school into disrepute and/or breach the integrity of the school's ethos. They

will also liaise directly with the police, Diocesan Education Board and/or local authority during relevant cases where families may bring the school's reputation into disrepute.

*Network Manager/Technical staff* (Local Authority Service Level Agreement)
Those with technical responsibilities are responsible for ensuring:

- 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 online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

*All Staff*
All staff have responsibility in setting a good example of internet use (see staff Code of Conduct). In addition, they must:

- All communication with children and parents / carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems e.g. Microsoft 365
- 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
- are aware of school rules with regards to photography and video of children, including knowing the children within their care for whom there is not explicit photo permission from primary caregivers
- they report any suspected misuse or problem to the Senior Leadership Team for investigation
- ensure all digital communications to families are conducted on a professional level and only carried out using official school systems (this includes not using social media under any circumstances from personal accounts to communicate about school issues).
- ensure that online safety issues are embedded in all aspects of the curriculum and other activities where relevant
- follow the Computing and PSHE long-term plans closely to ensure that age-appropriate e-safety issues are covered progressively
- monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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
- record e-safety incidents on CPOMS.

*Pupils:*

- first and foremost, remember to be kind to others online at all times.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- have age-appropriate understanding of internet research, copyright and issues around plagiarism
- Children in Year 3 and Year 4 have their own individual login and password for use for school devices. Children in EYFS & KS1 have an allocated, numbered iPad/laptop so users can be traced.

*Parents/carers*
**Working with Parents / Carers**

- We will build a partnership approach to online safety and will support parents/carers to become aware of and alert to the potential online benefits and risks for children by:

- Include details here e.g. providing information on our school website and through existing communication channels (such as official social media, newsletters etc.), offering specific online safety events for parents / carers or highlighting online safety at existing events
- Share which filtering and monitoring systems are in place with parents/carers and children
- Share what you are asking children to do online including which sites they might access

Who from the school or college will be interacting with their child online

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will, at relevant moments and using appropriate communication channels, ensure that parents understand these issues. 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
- e-safety at home
- legal guidelines around the use of social media (especially that social media channels almost always have a minimum age requirement of 13).
- social media for themselves, including not denigrating named individuals within the school such as children or staff.

**Policy Statements**
**Education - Children**

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-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.

E-safety should be a focus in all relevant areas of the curriculum and staff should reinforce online safety messages across the curriculum where possible. 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 as appropriate, both planned and ad hoc as necessary
- Children 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.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children should be helped to understand the principles from the acceptable use agreement (see appendix) and encouraged to adopt safe and responsible use both within and outside school/.
- 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 children are allowed to freely search the internet as part of a lesson, staff should be vigilant in monitoring the content of the websites the young people visit. However, there should always be some parameter of focus and children should not be allowed to simply 'browse the internet' without any direction or curriculum intent. Using search engines, for instance, may be done as part of a curriculum objective but staff must be cautious about its use. Staff are also reminded about the search engine risk assessment.
- There may be times when, for good educational reasons, students may need to research topics (e.g. 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. This decision must be made in conjunction with senior leaders.

- Staff must not use the internet in front of pupils without pre-planning – for instance, searching for items should not be done in front of children without this having been checked first away from children's view.

**Education – Parents/carers**

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 online 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.

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

- Curriculum activities
- E-safety training for families through our safeguarding consultants
- The school newsletter and other communication platforms between school and home
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications, e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

**Education & Training – Staff/Volunteers**

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 through our links with GEM Education. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff are made aware of online safety systems and the policy as part of their induction programme, ensuring that they fully understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring within school, as well as the school/ online safety policy and acceptable use agreements.
- The Online Safety Lead and/or other relevant staff will receive regular updates through attendance at external training events 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 meetings/briefings as appropriate.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

**Training – Governors**

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of the Teaching, Learning and Assessment Committee. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, Gosforth Schools Trust, National Governors Association, GEM or other relevant organisation (e.g. SWGfL).
- Participation in school/ training/information sessions for staff or parents.

**Technical – infrastructure/equipment, filtering and monitoring**

The school, through the Local Authority IT team, 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:

- 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 restrITed
- All users will have clearly defined access rights to school/ technical systems and devices.
- All users will be provided with a username and secure password by the Local Authority IT Service Desk who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. This includes Key Stage 2 children (whole-class accounts will be used for children younger than this.

- Local Authority IT Support 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 the Internet Watch Foundation CAIC list. Content lists for filtering are regularly updated. This is managed by the Local Authority IT Support team using Smoothwall filtering. There is a clear process in place to deal with requests for filtering changes. Smoothwall filtering includes terrorist and extremist material as per the Prevent agenda and other inappropriate websites.
- The school has provided enhanced/differentiated user-level filtering
- The Local Authority SLA team 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.
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place from the SLA 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 devices are protected by up to date virus software.
- Temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems can be arranged via UAM forms for all new users.
- An agreed policy is in place regarding the use of removable media (e.g. 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.

**Safeguarding Online Alerts**
NCC provides internet filtering for our school. The filtering solution, Smoothwall, is industry leading software which is updated on a nightly basis and blocks access to inappropriate content. Filtering can be modified on a school-by-school basis after discussion with NCC and all Internet access is logged and can be reported on by request.

We have purchased an additional filter called Smoothwall Monitor which provides safeguarding alerts to the DSL and other nominated staff members in school. The solution monitors individual user activity and uses artificial intelligence analytics to identify if it believes there is any behaviour you need to be concerned about. If there is, it sends an alert with date, time, username and a screenshot. Additionally, the software is able to identify changes in individual patterns of behaviour if they are logged on with a specific username.

We have web filtering in place as well and Google SafeSearch is enforced. Our web filters are updated constantly both by the vendor, and us. We can always bock websites where needed. We recognise that no web filtering system is 100% effective. The current Smoothwall web filter blocks out the expected categories e.g. violence, sex, gambling, hatred etc but is flexible enough to unblock sites or block sites as needed. No system can be expected to offer 100% protection, as the internet is constantly evolving, so constant vigilance is necessary. In addition, Smoothwall works with the HM Government Prevent agenda to block sites as identified by Prevent.

We have tailored our filters for our school. The governors have decided that they feel this is enough of a safeguard. Additionally, they felt that the Computing and PSHE curriculum that is offered in school teaches children about the risks of the internet. We agreed that we would continue to monitor this matter closely and make any necessary adjustments as the need arises. Regular checks to ensure filtering and monitoring systems are effective are undertaken, and the results, and required actions are logged. All staff receive regular training and updates.

"Smoothwall monitor" will identify not only websites accessed but each keystroke, word, phrase and sentence entered into any PC or Chromebook (not iPads as yet). Checking is undertaken initially by artificial intelligence and then passed for human analysis before being sent to the school.
IT lessons/use of technology is only undertaken with a member of staff present.

**Mobile Technologies**
Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, smartwatch, 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 which may include the school's learning platform and other cloud based services such as email and data storage. (Personally owned mobile technologies are not able to access the school's network.)

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

| | School Devices | | | | Personal Devices | | |
|---|---|---|---|---|---|---|---|
| | **School owned for staff** (e.g. laptop) | **School owned for staff (class tablets)** | **School owned for families** (e.g. home learning laptop) | **School owned for children** (iPads) | **Student owned** | **Staff owned** | **Visitor owned** |
| Allowed in school | Yes | Yes | No | Yes | *No* | *Yes* | *Yes* |
| Full network access | *Yes* | *No* | *No* | *No* | *No* | *No* | *No* |
| Internet only | No | Yes | *Yes (offsite)* | *Yes* | *No* | *No* | *No* |
| School network access | Yes | Limited (U: drive) | *No* | *No* | *No* | *No* | *No* |

Staff and visitors may bring their own devices into school and use them. These will not be able to access the school's network and no responsibility for their security or safety will be accepted by the school.

Personal devices, including phones and smartwatches, must not be used in classrooms and/or when in a child-facing position (with the exception of a smartwatch indicating the time).

Visitors are asked to turn off and not use their mobile phones in school for the safety and protection of staff and children.

**Use of digital and video images**
The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- As part of e-safety conversations, appropriate to the children's age and development, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/ events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in

some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/ policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/ equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school/ into disrepute.
- Children must not share, publish or distribute images of others without their permission. They may take and use photographs for educational purposes under the supervision of the class teacher.
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's surnames will not be used anywhere on a website or blog, particularly in association with photographs.
- Pictures and work will only be shared in accordance with parental permissions and data protection policies.
- Pictures must portray the school in a positive light if published.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and according to the Data Protection Policy and other related policies. Staff will particularly be aware of the following requirements from those policies.

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

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- Staff should not use USB sticks as a result of this and should use secure media (e.g. OneDrive through their school email).
- USB sticks must not be used by visitors, with all files emailed to a staff member and verified as per safeguarding recommendations.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

**Communications**

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:

| | Staff & other adults | Children |
|---|---|---|

| Communication Technologies | Allowed | Allowed at certain times away from children | Allowed for selected staff | Not allowed | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
|---|---|---|---|---|---|---|---|---|
| Mobile phones may be brought to the school/ | ■ | | | | ■ | | | |
| Use of mobile phones in lessons | | | | ■ | ■ | | | |
| Use of mobile phones/personal devices in social time | | ■ | | | ■ | | | |
| Taking photos on mobile phones/cameras | | | | ■ | ■ | | | |
| Use of school-owned other mobile devices e.g. tablets | | | ■ | | | | ■ | |
| Use of school/ email for personal emails | | | | ■ | ■ | | | |
| Use of messaging apps | | | | ■ | ■ | | | |
| Use of personal social media and blogs | | | | ■ | ■ | | | |
| Use of school social media | | | ■ | | ■ | | | |

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 can be monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Headteacher, 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 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.

**Social Media - Protecting Professional Identity**

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:

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to children, 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 or other organisation affiliated with the school (e.g. Diocesan Education Board, Local Authority, church links etc.)
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They are not 'friends' or 'followers' of parents and carers on social media platforms.
- If staff identify a post in a public forum that is by a family of the school, they never respond to messages and/or posts.

See also the Staff Code of Conduct

**Unsuitable/inappropriate activities**

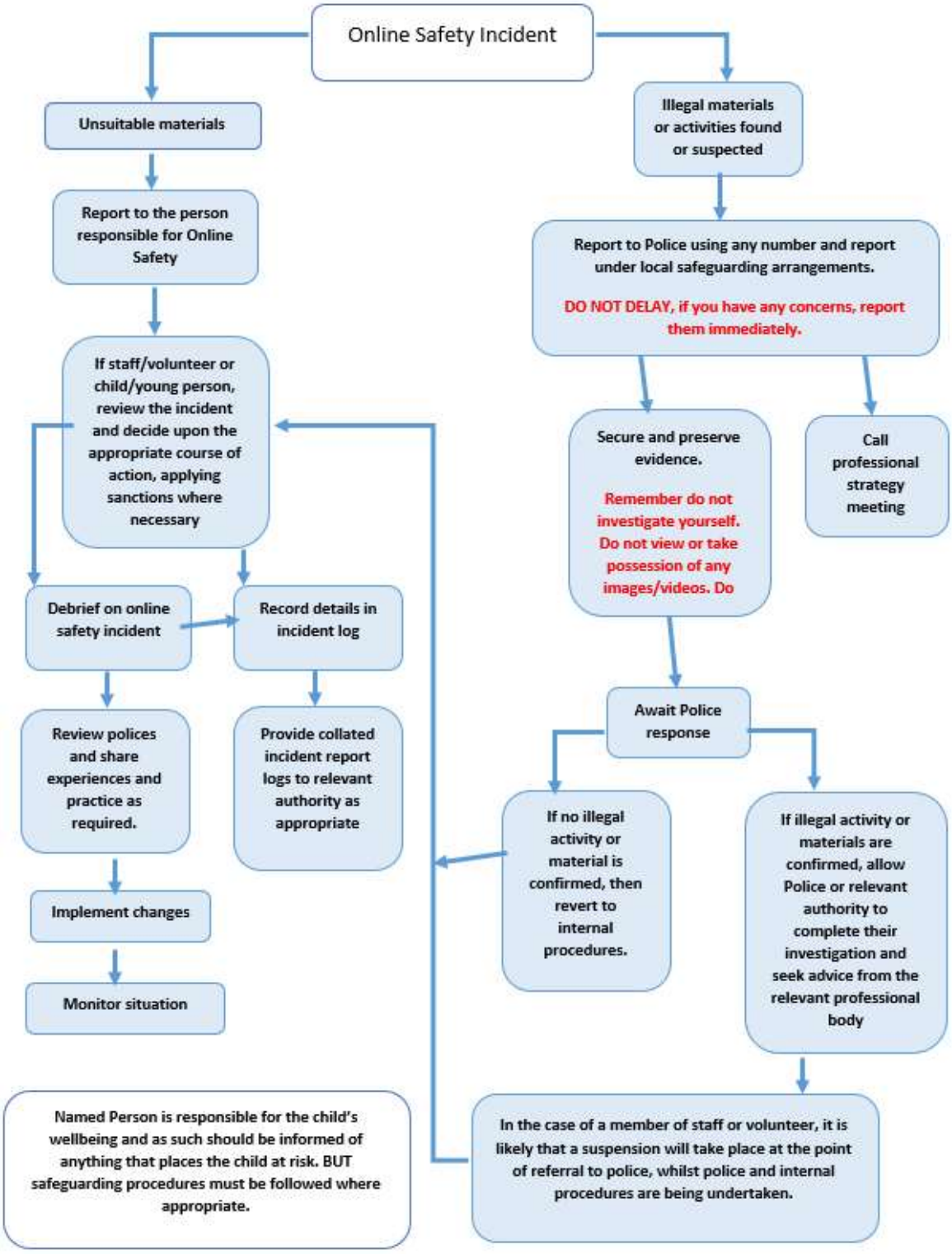
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| 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: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | 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:<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• 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/ | | | | | 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 | | | X | | |

**Responding to incidents of misuse**
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.

*Illegal Incidents*
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.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

**Other Incidents**
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.

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

- Have more than one senior member of staff 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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.

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.

**School actions & sanctions**
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:

| Children | Actions/Sanctions | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Refer to class teacher | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering/security etc. | Inform parents/carers | Removal of network/internet access rights | Warning | Further sanction e.g. exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | | X | X | X | | | | |
| Unauthorised use of non-educational sites during lessons | X | | | | | | X | |
| Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device | | X | | | X | | X | |
| Unauthorised/inappropriate use of social media/ messaging apps/personal email | | X | | | X | | X | |
| Unauthorised downloading or uploading of files | | | | X | | | X | |
| Allowing others to access school network by sharing username and passwords | X | | | | | | X | |
| Attempting to access or accessing the school/ network, using another student's/pupil's account | X | | | | | | X | |
| Attempting to access or accessing the school/ network, using the account of a member of staff | | | X | | X | X | | |
| Corrupting or destroying the data of other users | | X | X | | | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | | X | | X | | X | |
| Continued infringements of the above, following previous warnings or sanctions | | | X | | X | | | X |
| Actions which could bring the school/ into disrepute or breach the integrity of the ethos of the school | | | | | X | | X | |
| Using proxy sites or other means to subvert the school's/'s filtering system | | | | X | | | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | X | | X | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | | | X | | X | X | X | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | | X | X | | X | X | |

| | Actions/Sanctions | | | | | | |
|---|---|---|---|---|---|---|---|
| Staff | Refer to Headteacher | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | X | X | X | | | | |
| Inappropriate personal use of the internet/social media/personal email | X | | | X | X | | |
| Unauthorised downloading or uploading of files | X | | | X | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | | | X | | | X |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | | | | X | | |
| Deliberate actions to breach data protection or network security rules | X | | | X | | X | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | | | | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | | | | | X | |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils | X | | | | | X | |
| Actions which could compromise the staff member's professional standing | X | | | | X | | |
| Actions which could bring the school/ into disrepute or breach the integrity of the ethos of the school/ | X | | | | | | X |
| Using proxy sites or other means to subvert the school's/'s filtering system | X | | | X | | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | | | X | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | | X | | | X | |
| Breaching copyright or licensing regulations | X | | | X | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | | | | | X | |

| Date | Action | By whom? | Review date |
|---|---|---|---|
| July 2022 | New Policy | JB and agreed by FGB | |
| Jan 2023 | Reviewed | TLA | |
| Sept 2023 | Reviewed | KM, RL & Lonie Sebagh (link gov) | Sept 2024 |
| | | | |

**Appendix**
This policy is an adaptation from the SWGFL version, produced on the advice of the school's Computing consultants, GEM Education. Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:
http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

**Appendix 1: Staff Acceptable Use Agreement**

**Acceptable Use Agreement for Staff**

IT and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within school. To ensure that all adults within the school setting are aware of their responsibilities when using any form of IT all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provide positive role models to pupils for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the school equipment in an appropriate manner and for professional use in accordance with the e-Safety Policy
- I know that the School Uses Smoothwall to filter and monitor internet use
- I will not give out personal information (mobile phone number, personal e-mail address etc.) to pupils or parents
- I will only use the approved, secure e-mail system (name@schoolname.newcastle.sch.uk) for any school business
- I know that I should complete virus checks on my laptop, memory stick and other portable devices so that I do not inadvertently transfer viruses onto the school network or other IT equipment
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- USB sticks are only used for generic documents such as resource templates. I will not store any documents with parent/pupil names or personal pupil/parent data on USB sticks or external hard drives
- I will ensure school data is stored securely and used appropriately in accordance with school and other relevant policies
- I will not work in places where people can see personal parent/pupil d ata
- I will ensure that the screen is locked when I am away from the computer/laptop/iPad
- I will report any accidental misuse of school IT, or accidental access to inappropriate material, to the Head teacher immediately
- I will not connect any personal device (laptop, digital camera, mobile phone etc.), to the school network without authorisation from the Headteacher
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Head teacher
- I will ensure that my online activity, both in and outside school, will not bring myself or the school into disrepute (this includes postings on social networking sites and apps e.g. Facebook, Twitter, Instagram)

I have read, understood and agree to this code of conduct. I will support the safe and secure use of IT throughout the school. I am aware I may face disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name: _____

**Appendix 2: Children's Acceptable Use Agreements**

At Archbishop Runcie CE First School, these are Acceptable Use Rules, which are shared with pupils on a regular basis in class and assemblies and are available in the classrooms. Requiring pupils to sign these rules was deemed to be unnecessary by the governors and staff involved in formulating the policy.

***For EYFS to KS1:***
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
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.
I will only use my numbered iPad/laptop

***For KS2:***
I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

I will login to my school devices using my school username and password. I will keep these details private.

For my own personal safety:
- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will not use my own personal devices (mobile phones / USB devices etc.) in school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites in school.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, contact with parents and in the event of illegal activities, involvement of the police.

**Appendix 3:** ***(Confidential and internal only – not for publishing on the website.)***
Staff Social Media protocol

Staff use WhatsApp for informal school communications (whole staff and sub-groups). Staff can opt in or out of this communication forum. This is a positive forum that is mainly used for sharing information around practicalities and organisation.

By agreeing to join school-based WhatsApp communications, staff understand that:

- Group chats are not deemed private channels of communication and may be shared beyond those in the group; therefore, they must adhere to the policy above and must not bring the school, or anyone working here, into disrepute.
- Personal information will be shared with other group member e.g. phone numbers, status updates etc.
- No reference should be made to children or parents'/carers' names in staff group chats
- They do not engage in discussion on personal matters relating to themselves or other members of the school community
- The content of messages should remain professional, non-sexual and inclusive of all
- Security settings are regularly checked to minimise risk of loss of personal information
- Photographs should only be posted if the subject is aware that it was taken and will be shared (e.g. no photos should be taken without other staff members being aware)
- Messages should be positive and should never 'put down' or embarrass others
- Messages should not be sent after 10pm and not before 6am

I have read, understood and agree to this WhatsApp protocol. I am aware I may face disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name: _____