Wootton St Andrew's Church of England (VA) Primary School

January 2024

Digital Safeguarding Policy

Guidance

This policy is intended for staff and pupil use. It should be read alongside current legislation and other relevant school policies, including the Safeguarding and Child Protection Policy, Staff Conduct Policy, Anti-bullying policy and Home/School Agreement.

The Acceptable Use Agreement is issued on induction to the appropriate user for signature and collated by a designated member of staff.

The school should ensure that all persons, including Governors and pupils, who join the establishment mid-year are provided with the policy and agreement.

Vision and Rationale

At Wootton St Andrew's Church of England Primary School, we believe that computing offers children the opportunity to develop ways of thinking and understanding that empowers them in an ever-changing world. We are committed to enabling all pupils, regardless of background or ability, to achieve their full potential and to be equipped with the skills needed to be successful in their education and beyond. We recognise that children will have different starting points and different home access to technology but believe that this should not be a barrier to their success. We will offer children a broad and balanced curriculum which develops their use and understanding of computer-based technology, as well as using technology as a tool for learning. We will make use of technology to support children of different abilities wherever necessary. We encourage all members of the school community to develop positive attitudes towards computing. We aim to ensure that all users know how to stay safe when using digital devices and we put E-safety at the heart of everything we do. We will offer children a range of digital devices, areas of study and opportunities to put their learning into context.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the

internet

- The risk of being exposed to extreme views and groomed by those wishing to draw others into extreme activities
- The sharing/distribution of personal images with or without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents/carers and the wider community) to be aware and to assist in this process.

Online Safety

Online Safety - Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety Lead in this school is Mrs Zaitschenko who has been designated this role. All members of the school community have been made aware of who holds this post. It is the role of the E-safety Lead to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head and E-safety Lead and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy, whistle-blower, equality and PSHE.

Online Safety in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

- The school has a framework for teaching internet skills in Computing lessons
- The school provides opportunities within a range of curriculum areas to teach about Online Safety
- Educating pupils about the online risks that they may encounter both inside and outside school is done at the start of each term and whenever opportunities arise and as part of the Online Safety curriculum
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

Online Safety Skills Development for Staff

- Our staff receive regular information and training on Online Safety and how they can promote the 'Stay Safe' online messages. Appropriate courses on EduCare are completed and information review
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)

- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas

Managing the School Online Safety Messages

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used
- The Pupil Acceptable Use Policy will be introduced to the pupils at the start of each school term
- Online Safety posters will be prominently displayed

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. We cascade Online Safety information onto parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks. The school website includes additional advice for parents in managing online safety.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school and as part of the home/school agreement pack at the start of the school year
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on the school website)
- Parents/carers are expected to sign a Home School agreement stating their support of the school and its policy
- The school disseminates information to parents relating to Online Safety where

appropriate in the form of leaflets, newsletters and sending texts to direct them to features added to the school website.

Internet Access

The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

It is not the school's policy to 'shut down' internet access but rather to help children develop the skills needed to keep themselves safe online. However, internet access is filtered in order to limit the risk posed to pupils. It is recognised that no filtering system can be completely secure and all users are instructed to inform the E-safety lead of any breaches.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites could be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources
- LA provide differentiated filtering for all users

Internet Use

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Staff must not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Wootton St Andrew's C of E Primary school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity is monitored and explored further if required
- The school does not allow pupils access to internet logs
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-safety Lead or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the E-safety leader.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used
- Users must not interfere with any anti-virus software installed on school Computing equipment that they use
- If staff machines are not routinely connected to the school network, staff must make provision for regular virus updates by ensuring that they regularly connect to the internet
- If a user suspects there may be a virus on any school computing equipment, they must stop using the equipment and contact the E-safety Lead or IT support, who will advise them on what actions to take and be responsible for advising others that need to know

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits for communication and collaboration.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000
- Staff must inform the E-safety Lead if they receive an offensive e-mail

Sending e-Mails

- Staff should use their own school e-mail account so that they are clearly identified as the originator of a message
- Users should keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Users should check their e-mail regularly
- Users must never open attachments from an untrusted source
- Users should not use the e-mail systems to store attachments. They should detach and save business related work to the appropriate shared drive/folder

Managing Other Web 2.0 Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we

encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school unless set for curriculum purposes
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests)
- Our pupils are advised that, if they do have online profiles, these should be set to maximum privacy and they should deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Pupils are asked to adhere to age recommendations on social media sites
- Our pupils are asked to report any incidents of Cyberbullying to the school, even if they occur outside school time

Social Media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses an app to communicate with parents and carers. Certain named staff are responsible for all postings on these technologies
- Pupils are not permitted to access their social media accounts whilst at school. Pupils are reminded about age limits associated with such media accounts and encouraged to follow these
- Staff, governors, pupils, parents and carers are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Youth Produced Sexual Imagery

Also known as 'Sexting', Youth Produced Sexual Imagery (YPSI) refers to indecent images of anyone under the age of 18, produced by a person under the age of 18. It is illegal for a person to create, share or possess an indecent image of anyone under the age of 18. However, most police forces regard YPSI as a safeguarding issue and will not prosecute unless the incident is part of a series of offences or involves other aspects such as blackmail. When dealing with an incident, staff can refer to government advice found in https://www.gov.uk/government/uploads/system/uploads/attachment data/file/551575/

6.2439 KG NCA Sexting in Schools WEB 1 .PDF

- In an age appropriate manner, we will teach children about the risks and consequences of YPSI, including through our SRE teaching and the Big Talk.
- Children will be taught about the risks associated with the ease of sharing photographs, the loss of control when they are put on social media and the permanence of images put online.
- Children are helped to consider the appropriateness of any images they produce and share using the rule: 'Don't create or share images that you wouldn't want your mum/ grandma/ teacher etc to see.'
- If staff are concerned that there may be an incident of YPSI they must report the issue to the Designated Safeguarding Lead who will inform parents (unless this would put the child at risk) and, if necessary, the police. If a child is deemed to be in immediate danger, the police will be informed straight away. In other incidents, it may be necessary to contact CEOP (Child Exploitation and Online Protection) who can investigate the issue and can also assist in the removal of any indecent material from the web.
- Staff, should not view YPSI unless absolutely necessary. Under these circumstances, the DSL should follow government guidance, including ensuring that there is more than one member of staff present (although the other staff do not need to view the image) and that they are in a private location such as the Headteacher's office. Ideally, the member of staff viewing the image should be of the same sex as the young person.
- Under no circumstances should staff copy or store YPSI as this is a criminal offence

Staff Professional Responsibilities

These are a clear summary of **professional responsibilities related to the use of IT** which has been endorsed by unions, such as: NEU, NASWT, ATL, UNISON.

For your own protection we advise that you:

- Be sure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies
- Do not talk about your professional role in any capacity when using social media such as Facebook
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera
- Do not give out your own personal details, such as mobile phone number, e-mail address or social network details to pupils, parents, carers and others
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately
- Only take images of pupils and/or staff for professional purposes, in accordance with school policy and with the knowledge of SLT
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Be sure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute
- You have a duty to report any e Safety incident which may impact on you, your professionalism or your organisation

Password and Password Security

Passwords

- **Users must always use their own** personal passwords
- Users must make sure they enter their personal passwords each time they logon. They must not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Users should change passwords whenever there is any indication of possible system or password compromise
- **Users must only disclose their personal password to authorised IT support staff when necessary, and never to anyone else.** They should ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Staff should never tell a child or colleague their password**
- **If users are aware of a breach of security with their password or account they must inform the E-safety Lead immediately**
- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data and have a different level of filtering. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends, unless they need to share with a member of staff or the IT support. Staff and pupils are regularly reminded of the need for password security.

- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS systems including ensuring that passwords are not shared and are changed periodically
- Individual staff users must also make sure that workstations are not left unattended and are locked

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. The school will ensure that all user accounts are disabled once the member of the school has left.

Safe Use Of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, and within the home/school agreement at the start of the school year, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and app
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that no objections have been given for work to be displayed.

Storage of Images

- Images/films of children are stored on the school's IT programmes
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource

Webcams

- We do not use publicly accessible webcams in school

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with endpoints beyond the school
- No part of any video conference is recorded in any medium without the written consent of those taking part

School IT Equipment including Portable and Mobile IT and Removable Media

School IT Equipment

- It is recommended that schools log IT equipment issued to staff and record serial numbers as part of the school's inventory
- Visitors are not allowed to plug their IT hardware into the school network points (unless special provision has been made). If they require internet access,

they may be connected to the wireless network at the discretion of the Digital Lead or IT support staff

- All staff are asked to ensure that IT equipment is kept physically secure
- Users must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that users save their data on a frequent basis to the school network. Users are responsible for the backup and restoration of any data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable device. If it is necessary to do so the local drive must be encrypted
- On termination of employment, resignation or transfer, all IT equipment must be returned to the Headteacher. Users must also provide details of all system logons so that they can be disabled
- It is user's responsibility to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

Portable & Mobile IT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey
- Ensure portable and mobile computing equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the IT support team, fully licensed and only carried out by your IT support
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible,

must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, tablets/iPads and games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device
- The school is not responsible for the loss, damage or theft of any personal mobile device
- Personal devices must not be used with the children for any purpose
- Personal devices should not be used to take photos, videos or sound recordings of the children
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Removable Media

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the IT support staff

Monitoring and Security

Authorised IT support staff may inspect any computing equipment owned or leased by the School at any time without prior notice.

IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School Computing; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

IT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised staff.

Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for Computing Acceptable Use
- Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile computing equipment or removable storage media in unattended vehicles. Where this is not possible, it should be kept locked out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared devices are used.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school Computing hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the local authority Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law
- Prosecute those who commit criminal offences under the Act
- Conduct audits to assess whether organisations processing of personal data follows good practice
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of computing equipment must be immediately reported to the school's E-safety Lead. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy noncompliance must be reported to the head teacher.

Please refer to the section Incident Reporting, Online Safety Incident Log & Infringements.

Incident Reporting, Online Safety Incident Log and Infringement

Incident Reporting

Any issues relating to Online Safety should be made to the E-safety lead. Where concerns relate to the safety of a child, these should be dealt with in accordance with

the school's Child Protection Procedures. Where concerns relate to cyber bullying, these should be dealt with in relation to the school's behaviour policy. Wherever applicable, staff should liaise with parents to deal with online safety issues.

Details of any online safety issues should be kept within the children's profile and a copy should be given to the E-safety lead so that issues can be monitored and any patterns noted. The school will deal with the incident straight away and then look at ways to prevent it from recurring or spreading e.g. raising awareness, blocking and reporting content, informing the police if illegal activity is involved.

Issues regarding Online Safety concerns should, where appropriate, inform the planning of Online Safety teaching to ensure that children know how to deal with any incidents. For example, if an issue relating to cyberbullying occurs, a teacher will address how to deal with, and prevent, cyberbullying within their Online Safety lessons or PSCOs will deliver whole school presentations.

Misuse and

Infringements

Complaints

Complaints and/or issues relating to Online Safety should be made to the E-safety Lead or Headteacher. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-safety Lead
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety Lead and depending on the seriousness of the offence; investigation by the Headteacher

Review Procedure

There will be on-going opportunities for staff to discuss with the E-safety Lead any Online Safety issue that concerns them. This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

References

- CEOP (Child Exploitation and Online Protection centre)
- https://www.thinkuknow.co.uk/
- **Internet Watch Foundation -** report inappropriate Web sites https://www.iwf.org.uk/
- Childnet
- Parents Guide on Internet usage http://www.childnet.com/parents-and-carers
- Internet Matters - helping parents keep their children safe online
- https: //www.inter netmatters.org/
- **Copyright** www.templetons.com/brad/copymyths.html - Covers the main aspects of copyright of digital materials, US-based but relevant.

Approved by:	Headteacher	R.Zaitschenko	Date Approved:	January 2024
	Chair of Governors:	Rev.A.Wright	Review Date:	January 2025
	Governors:	K.Hewson, A.Morgan		