Willenhall
Community
Primary School

E-safety policy

Owner:	Computing Lead	Published date:	March 2023
Approved by Headteacher:	J McLean	Date:	19/10/2023
Approved by Governors:	P&S Committee – L Tovey	Date:	19/10/2023
Date to be reviewed:	September 2024		

Contents

1. Aims:

IT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Computing Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of IT within our society as a whole.

Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile / Smart phones and watches with functionality including: text, video, web, audio, music, global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying and grooming.

At Willenhall Community Primary School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools (updated 2023)
- Preventing and tackling bullying and cyber-bullying: advice for head teachers and school staff
- Relationships and sex education

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy is intended to be supported by the school's Acceptable Use Policy for staff, governors, visitors and pupils (see appendices). Its purpose is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection and Safeguarding, Health and Safety, Behaviour & Restraint and Anti-Bullying, and particularly to the curricular for PHSE and SRE. See section 19 for a full list of supporting policies.

3. Roles and Responsibilities

3.1. The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet.

3.2. The Head Teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3. The Computing Lead / E-Safety co-ordinator

In our school the role of e-safety co-ordinator falls within the scope of the Computing Lead. The named e-Safety co-ordinator in our school is Miss Rebecca Archer who has been designated this role as a leader of Computing in school. All members of the school community have been made aware of who holds this post.

It is the role of the Computing Lead to keep abreast of current issues and guidance through organisations such as Coventry LA, CEOP (Child Exploitation and Online Protection), UKCCIS and Childnet.

The Computing Lead takes lead responsibility for online safety in school, in

particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, IT Consultant and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing board
- Providing SLT and Governors with an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.
- This list is not intended to be exhaustive.

3.4. The IT Consultant

The IT Consultant is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- This list is not intended to be exhaustive.

3.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the Computing Lead to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

3.6. Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet /mobile devices in an appropriate way. We encourage and support parents to be fully involved with promoting IT both in and outside of school while appreciating the benefits provided by technologies generally.

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet on an annual basis
- Make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website)
- Notify a member of staff or the head teacher of any concerns or queries regarding this policy

Parents and carers are encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school
- use of digital and video images

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

Healthy relationships – Disrespect Nobody

Keeping children safe online- NSPCC

Online and mobile safety- Childline UK

3.7. Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. IT skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of INSET or through staff meetings.
- The Computing Lead ensures that staff have an up to date awareness of e-

safety matters and of the current school e-safety policy and practices.
- New staff receive information on the school's Acceptable Use Policy and e-Safety 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 IT and know what to do in the event of misuse of technology by any member of the school community.
- All staff are expected to incorporate e-Safety activities and awareness within the Computing, PSHE and SRE curriculum areas.

5. Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the Internet and/or related technologies are used. This is particularly reinforced in PSHE and SRE lessons in relation to cyber-bullying and to grooming.
- The e-Safety and Acceptable Use of IT policies will be introduced to the pupils annually, initially at the start of each new school year, in school assemblies and during Safer Internet Day.

6. Computing in the Curriculum

IT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be delivered to the pupils on a regular and meaningful basis. E-Safety is threaded through our curriculum and we continually look for new opportunities to promote its importance.

- The school provides opportunities within a range of curriculum areas to promote e-Safety. Children are reminded of e-Safety rules when using the internet across the curriculum.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and formally as part of the curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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 ChildLine.
- Pupils are taught to critically evaluate materials and apply appropriate skills when using search engines through cross curricular teacher models, discussions and via the Computing curriculum (for example in Year 2 when carrying out topic research or in Year 5 when creating their own website).
- PSHE & SRE lessons provide the opportunity to discuss issues relating to

cyber-bullying and Internet grooming (e.g. through respect for others and appropriate / positive relationships). These lessons can equip pupils with the knowledge to keep safe from harm.

7. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, not even with their friends. Staff and pupils are regularly reminded of the need for password security and can refer to the password handout for advice (see appendices) on devising secure passwords.

- All users read **and sign** an Acceptable Use of IT agreement annually to demonstrate that they have understood the school's e-Safety policy.
- Users are provided with an individual email and Learning Platform log-in username. From Key Stage 1, they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to their teacher who will inform the Computing Lead.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and Learning Platform, including ensuring that passwords are not shared and are changed when necessary (see previous point).
- Individual staff users must also make sure that workstations are not left logged-on.
- Due consideration should be given when logging into Google Classroom, the school's online Learning platform, to the browser/cache options on a shared computer.
- In our school, all IT password procedures are the responsibility of the Computing Lead and all staff and pupils are expected to comply with the policies at all times.

8. General Data Protection (GDPR) and e-safety

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

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage

devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher and Data Protection Lead (Office Manager).
- Any data taken off the school premises must be done only with permission from SLT.
- Data can only be accessed and used on school computers or authorised laptops. Staff are aware they must not use their personal devices for accessing any school or pupil data.
- The school network is backed up internally using a secure remote back up facility.
- Only the Head Teacher and Deputy Head Teacher, the Safeguarding Team and Admin Team have remote access to school data.
- In the event of a data breach, the school will notify the LA Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

9. Managing the Internet

The Internet is an open communication medium, available to all, 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. In our school access to the Internet is via the LA internet grid. Internet is logged and the logs are randomly but regularly monitored by IMPERO. Whenever any inappropriate use is detected it will be followed up.

- In our school students are not allowed unsupervised access to the Internet.
- Staff will preview any recommended sites before use with students.
- Raw image searches (e.g.: Google) are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible, links from the school learning platform will be provided.
- 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.

10. Infrastructure

- The school uses monitoring software (Impero) purchased through the Coventry Local Authority.
  Upon request, web-based activity can be monitored and recorded.
- School Internet access is controlled through the Impero web filtering service.
- In addition, our school also manages some bespoke web filtering via the Firewall provided by the Local Authority which is the responsibility of the Computing Lead.
- Willenhall Community Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, 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 can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off and the incident reported immediately to the Computing Lead or Head Teacher. The offending URL will be reported to the school IT Consultant.
- Anti-Virus protection is provided by the LA Norton Antivirus and is set to automatically update on all school machines. This is the responsibility of the Computing Lead and IT Consultant.
- In addition, staff laptops used at home can also be protected by monitoring software.
- Pupils and staff are not permitted to download programs on school equipment without prior permission from the Head Teacher, Computing Lead or IT Consultant.
- If there are any issues related to viruses or anti-virus software, the Head Teacher, Computing Lead and IT Consultant should be informed.

11. Managing other communication & networking technologies

The Internet includes a wide range of communication and networking tools and sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. Social Media 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 denies access to social networking sites to pupils

within school.

- All pupils are advised to be cautious about the information given by others on sites, 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 sites 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 such sites 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 about the lawful age restrictions on having profiles on Social Media.
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying to the school.
- Pupils are introduced to a variety of Internet communication tools within a safe context.
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools with pupils and parents (e.g. Facebook, Myspace, Twitter, email etc.).

12. 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. Many existing mobile technologies (such as portable media players, gaming devices, Smart phones, smart watches etc.) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

12.1. Personal Mobile devices (including phones and smart watches)

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 or parent/carer using their personal device. At all times the device must be switched to silent mode.

- Pupils are not allowed to bring personal mobile devices/phones to school unless specific permission is sought from the Head Teacher or Deputy. (Year 5 and 6 pupils – see Mobile Devices policy). Pupils will be expected to sign a contract if they bring in a mobile device including phones, smart watches etc.

- Technology may be used, for educational purposes, as mutually agreed with the Head Teacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed in any context.
- Permission must be sought before any image, video or sound recordings are made on these devices of any member of the school community.
- Capturing images and video is not allowed by students or staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

12.2. School provided Mobile devices (including phones)

- The sending of inappropriate messages between any members of the school community is not allowed.
- Where the school provides mobile technologies (e.g. phones, laptops, etc.) for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop, iPad or Chromebook for staff, only this device may be used to conduct school business outside of school.

13. Managing email

The use of email within most schools is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'. In order to achieve this, pupils must have experienced sending and receiving emails.

- The school gives all staff an individual email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff email should be used for all school business.
- Staff should regularly review and delete their emails to ensure compliance with data protection regulations.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

- Staff sending emails to external organisations, parents or pupils are advised to cc. the Head Teacher, line manager or designated office account.
- Staff email is subject to mail scanning check
- The forwarding of chain letters is not permitted in school.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Staff must inform (the Head Teacher, Computing Lead or their line manager if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work initially in Year 2. This is then developed in KS2.
- Pupils must immediately tell a teacher or trusted adult if they receive an offensive message and keep the offending message(s) as evidence.

14. Remote/Home Learning

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and online learning platform (Google Classroom).
- We expect pupils to follow the same principles, as outlined in the school's Acceptable Use Policy, whilst learning at home.
- If our school chooses to communicate with pupils via video conferencing staff should follow the guidelines outlined in the school's Video Conferencing Policy.
- Any concerns including inappropriate behaviour occurring on any virtual platform must be recorded and reported via the school's Child Protection Online Management System (CPOMS) to the school's Designated Safeguarding Lead.

15. Safe Use of Images / Video

15.1. Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily misused. We must remember that it is not ever 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 / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g. mobile phones and cameras), to record images of pupils, this includes when on field trips.

15.2. Consent of adults who work at the school

- Parents must seek permission to take photos / video school events, and must

agree to NOT post images / video on the Internet.
- Video captured by school staff, are stored on the secure school server for as long as is required and made available on the school website or learning platform.

15.3. Publishing pupil's images

On a child's entry to the school, all parents/guardians will be asked to give signed permission to use their child's work/photos/ video in the following ways:

- on the school website and social media sites (Twitter, YouTube)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video
- for internal displays and workbooks or journals
- in the local paper (sent using traditional methods or electronically)
- for staff training purposes within the federated schools
- in group photos taken by the school's chosen photographer

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, e.g. divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given in order for it to be deemed valid.

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

Video streamed from the service is always set to "private".

Only the IT Consultant and Admin staff have authority to upload to the public website.

15.4. Storage of Images / Video

- Images/video of children are stored on the school's network on the 'Media Server'.
- Pupils and staff are not permitted to use personal portable media (e.g. USB storage devices) for storage of images.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of school.
- Images/video of pupils are deleted as soon as the purpose no longer exists and at regular intervals throughout the academic year, this is the responsibility of the person who created the images.
- Class Teachers have the responsibility for ensuring that images and recordings are retained in line with the school's record retention schedule.

15.5. Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to

this are the Admin staff, Head Teacher and Site Manager. For further information, please see the school's CCTV policy.

- We do not use publicly accessible webcams in school other than for special projects such as nature cams which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes, (e.g. monitoring hens' eggs). Images of children/adults are never broadcast without parental permission.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Notification is given when a webcam is in an area.

15.6. Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues that affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via one of the Designated Safeguarding Leads). Concerns should be forwarded to the LA Prevent Team for assessment for further action.

Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

16. Misuse and Infringements

16.1. Complaints

Complaints relating to e-Safety should be made to the Computing Lead or Head Teacher following the school's Complaints policy.

16.2. Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Computing Lead/IT Consultant and Head Teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head Teacher, and depending on the seriousness of the offence may lead to:
    - Reporting to the Child Protection Officer
    - Investigation by the Head Teacher or LA
    - Immediate suspension
    - Dismissal
    - Involvement of police
- Users are made aware of sanctions relating to the misuse or misconduct as outlined in the Disciplinary Policy.

17. Equal Opportunities

Pupils with additional needs

- The school endeavours work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the school's rules.
- Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

18. Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the Computing Lead any issue of e-Safety 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. This policy has been read, amended and approved by the staff, head teacher and governors, please see front cover for dates.

19. Supporting policies

The following school policies and procedures should also be referred to:

- Acceptable Use of IT Policy (separate policies for staff and pupils)
- Anti-Bullying Policy
- Behaviour Policy
- CCTV policy
- Child Protection and Safeguarding policy
- Data Protection policies & record retention schedule
- Guidance on Safer Working Practice
- General Data Protection Regulation Privacy Notice
- Mobile Devices policy
- Photography policy
- Remote Learning policy
- Social Media guidance
- Staff Code of Conduct
- Video Conferencing policy
- Whistleblowing policy
- Working from Home policy

20. Appendices

20.1. Acceptable Use of IT for staff, governors, volunteers

policy_Acceptable Use of IT.pdf

20.2. Acceptable Use of IT for pupils

policy_Pupil Acceptable Use of IT

20.3. Setting secure and memorable passwords

handout - passwords.pdf