יבנה

Yavneh

Primary School

Yavneh Primary School
E – Safety Policy

E-Safety Policy

1. Introduction to E-Safety

We believe here at Yavneh Primary School that the use of computing in our school brings great benefits to the pupils, families and staff.
Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications.

1.1 Whilst exciting and beneficial both in and out of the context of education, much ICT, 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.

1.2 At Yavneh 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.

1.3 Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

1.4 Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.5 Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2. Monitoring

2.1 Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

2.2 ICT 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 ICT; 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.

2.3 ICT 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.

2.4 All monitoring, surveillance or investigative activities are conducted by ICT 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.

2.5Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3. Breaches

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

3.2Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure

4. Incident Reporting

4.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher.

Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non- compliance must also be reported to the Headteachers.

4.2 Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

5. Acceptable Use Agreements:

Yavneh Primary School

Yavneh Primary School

Foundation Stage Safe Online Agreement

S 	*I will only use the Internet with an adult. I will only use my Teams account in school, with my teachers.*
A 	*I will only click on icons and links when I know they are safe.*
F 	*I will only send friendly and polite messages. I will not share personal information, like my name, address or telephone number.*
E 	*If I see something I do not like on a screen, I will always tell an adult.*

My Name:

Parent Name:

Date:

Yavneh Primary School

KS1 Safe Online Agreement

S 	I will only use the Internet with an adult. I will only use my Teams account in school, with my teachers.
A 	I will only click on icons and links when I know they are safe.
F 	I will only send friendly and polite messages. I will not share personal information, like my name, address or telephone number.
E 	If I see something I do not like on a screen, I will always tell an adult.

My Name:

Parent Name:

Date:

Yavneh Primary School

KS2 Pupil Acceptable Use Agreement

All pupils must follow the rules in this policy when using:
school computers or any chat rooms/websites out of school.

Pupils that do not follow these rules may find that:

- *They are not allowed to use the computers at school.*
- *They can only use computers at school if they are closely monitored.*
- *There will be a meeting held with them and their parents about their behaviour.*

Responsible Online Use	
1	*I will only use polite language and be kind when using the computer or online, at home or at school.*
2	*I will not send messages or content during or after school hours to anyone involved with school which may upset or offend them or which says anything rude or unkind.*
3	*I am aware that some websites and social networks have age restrictions and I should respect this.*
4	*I must not tell anyone my name, where I live or my telephone number over the internet. I will never arrange to meet someone I have only ever previously met on the internet.*
5	*I must not tell anyone my usernames or passwords except my parents or school adults.*
6	*I will tell my teacher or parent if I receive any messages that make me feel uncomfortable.*
7	*I will try not to damage any computing equipment.*
8	*I will not damage or destroy the work of another person by deleting it, or in any other way.*
9	*If I find something that I think I should not be able to see, I must tell my teacher or parent straight away and not show it to other pupils/ children.*
10	*I must log off after I have finished using the computer.*
11	*I will use my account responsibly:* • *I will NOT share my login details with anybody except my teacher* • *I will only log into my own Teams account* • *I will only use my account in school, during school hours* • *I will communicate politely and respectfully* • *I will not share my personal information from my Teams account* • *I understand that my account is a school account and will be monitored by my teachers at school regularly*

I agree to follow the school rules when using the school computers. I will use computers sensibly and follow the rules explained by my teacher.
I agree to report anyone not using computers sensibly or being inappropriate online to my teacher/ parent.
I agree to tell my teacher/ parent if I see websites that make me feel unhappy or uncomfortable.
If I do not follow the rules, I understand that this may mean I might not be able to use the school computers.

Date: _____

*Pupil Name:*_____ *Pupil Signature:*_____

*Parent Name:*_____ *Parent Signature:*_____

Yavneh Primary School

Acceptable Use Agreement Form for Parents

AUA review Date:	**September 2024**
Date of next Review:	**September 2025**
Reviewed by:	**Headteacher**

Internet and ICT: As the parent of the child(ren) named below, I grant permission for the school to give my *daughter/ son* access to:

- the internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school

I know that my daughter or son has signed an Acceptable Use Agreement form.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep children safe and to prevent children from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching Online Safety skills to children.

I understand that the school can, if necessary, check my child's computer files and the internet sites they visit at school and if there are concerns about my child's Online Safety or behaviour they will contact me.

I understand that the school uses a safe search engine Kids Rex which I can also use at home. http://www.kidrex.org/

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and or share online, photographs/videos of other children at school events

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's Online Safety.

Name of child: _____

Parent signature: _____

Date: ___/___/___

Yavneh Primary School
Acceptable Use Agreement for Governors

AUA review Date: **September**
Date of next Review: **September**
Reviewed by: **Headteacher**

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This Staff Acceptable Use Agreement covers use of digital technologies in school: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems within our school.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body
- I will not reveal my password(s) to anyone
- I will lock or log off my computer when it is left unattended
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it
- I will not allow unauthorised individuals to access email / internet / intranet / network, or other school systems
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols
- I will not engage in any online activity that may compromise my professional responsibilities
- I will only use the approved, secure email system(s) for any school business
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Online Safety Officer
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed
- I will not publish or distribute work that is protected by copyright
- In my role as a governor I will not use personal digital cameras, Smart Watches, iTouches or camera phones for taking and transferring images of children or staff
- I will not put images of children online which are labelled with their names
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs
- I will access school resources remotely (such as from home) only through school approved methods and follow e-security protocols to access and interact with those materials
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location
- I understand that data protection policy requires that any information seen by me with regard to staff or children information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority
- I understand that all internet usage / and network usage can be logged and this information could be made available to my manager on request
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or children), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school
- I will not use the schools' internet facility for financial gain
- I understand that failure to comply with this agreement could lead to disciplinary action

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Headteacher)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

6. Computer Viruses

7.1 All files downloaded from the Internet, received via e-mail or on removable media (e.g. CD, memory sticks or other removable storage media) must be checked for any viruses using school provided anti-virus software before using them

7.2 Never interfere with any anti-virus software installed on school ICT equipment that you use

7.3 If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

7.4 If you suspect there may be a virus on any school ICT equipment, stop using the equipment and inform Mrs Collins immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

8 Security

8.1 The School gives relevant staff access to its Management Information System, with a unique ID and password

8.2 It is the responsibility of everyone to keep passwords secure

8.3 Staff are aware of their responsibility when accessing school data

8.4 Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

8.5 Staff keep all school related date secure. This includes all personal, sensitive, confidential of classified data

8.6 Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

8.7 Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

8.8 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. Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

9 Disposal of Redundant ICT Equipment Policy

9.1 All redundant ICT equipment will be disposed off through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

9.2 All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

9.3 The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

9.4 The school's disposal record will

include: Date item disposed of

9.5 Authorisation for disposal, including:

Verification of software licensing

9.6 Any personal data likely to be held on the storage

media How it was disposed of e.g. waste, gift, sale

9.7 Name of person & / or organisation who received the disposed item

9.8 If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

9.9 Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

10 e - Mail

10. 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 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 e-mail in relation to their age and good network etiquette; 'netiquette'.

10.1 The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e- mails and avoids the risk of personal profile information being revealed

10.2 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 e-mail histories can be traced. The school email account should be the account that is used for all school business

10.3 Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

10.4 All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

10.5 Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacherss, line manager or designated account

10.6 Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

10.7 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. You must therefore actively manage your e-mail account as follows:

10.8 Delete all e-mails of short-term value

10.9 Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

10.10 The forwarding of chain letters is not permitted in school. However the school will set up a dummy account (specify address) to allow pupils to forward any chain letters causing them anxiety. No action will be taken with this account by any member of the school community

10.11 All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

10.12 Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e- mail

10.13 Staff must inform (the Headteachers) if they receive an offensive e-mail

10.14 Pupils are introduced to e-mail as part of the Computing curriculum

10.15 However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

10.16 The use of personal Internet based webmail service for sending, reading or receiving business related e-mail is not permitted

11 Sending e-Mails

11.1 Use your own school e-mail account so that you are clearly identified as the originator of a message

11.2 Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

11.3 Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

11.4 School e-mail is not to be used for personal advertising

12 Receiving e-Mails

12.1 Check your e-mail regularly

12.2 Never open attachments from an untrusted source

12.3 Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

12.4 The automatic forwarding and deletion of e-mails is not allowed

13 e-mailing Personal, Sensitive, Confidential or Classified Information

13.1 Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing confidential data is not recommended and should be avoided where possible

13.2 Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)

13.3 Send the information as an encrypted document **attached** to an e-mail

13.4 Provide the encryption key or password by a **separate** contact with the recipient(s)

13.5 Do not identify such information in the subject line of any e-mail

13.6 Request confirmation of safe receipt

14 Equal Opportunities

Pupils with Additional Needs

14.1 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' eSafety rules.

14.2 However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

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

15 eSafety - Roles and Responsibilities

15.1 As eSafety is an important aspect of strategic leadership within the school, the Headteachers and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is **Caroline Field**. All members of the school community have been made aware of who holds this post.

15.2 Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

15.3 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 (including the anti-bullying) and PHE policies.

16 eSafety Skills Development for Staff

16.1 Our staff receive regular information and training on eSafety issues

16.2 New staff receive information on the school's acceptable use policy as part of their induction

16.3 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

16.4 All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

17 Managing the School eSafety Messages

17.1 We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

17.2 The eSafety policy will be introduced to the pupils at the start of each school year

17.3 eSafety posters will be prominently displayed

18 Incident Reporting, eSafety Incidents & Infringements

18.1 Incident Reporting - Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher and on CPOMS.

19 Misuse and Infringements

19.1 Complaints

19.1.1 Complaints and/ or issues relating to eSafety should be made to the Headteachers. Incidents should be logged and appropriate action taken.

19.2 Inappropriate Material

19.2.1 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to Headteachers.

19.2.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteachers, depending on the seriousness of the offence; investigation by the Headteacherss, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

20 Internet Access

20.1 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. Whenever any inappropriate use is detected it will be followed up.

21 Managing the Internet

21.1 Staff will preview any recommended sites before use

21.2 Raw image searches are discouraged when working with pupils

21.3 If Internet research is set for homework, specific sites will 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

21.4 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

21.5 All users must observe copyright of materials from electronic resources

22 Internet Use

22.1 You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience

22.2 Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

22.3 On-line gambling or gaming is not allowed

22.4 It is at the Headteachers discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

23 Infrastucture

23.1 Yavneh 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

23.2 Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

23.3 The school does not allow pupils access to internet logs

23.4 If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

23.5 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

23.6 If there are any issues related to viruses or anti-virus software, the network manager should be informed

24 Parental Involvement

24.1 We believe that it is essential for parents to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents and seek to promote a wide understanding of the benefits related to ICT and associated risks.

24.2 Parents and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy

24.3 Parents are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

24.4 Parents 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 school website)

24.5 The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Website/ Virtual Learning Environment postings
- Newsletter items
- Virtual Learning Environment training

25 Passwords and Password Security

25.1 Passwords

25.2 Always use your own personal passwords to access computer based services

25.3 Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

25.4 Staff should change temporary passwords at first logon

25.5 Change passwords whenever there is any indication of possible system or password compromise

25.6 Do not record passwords or encryption keys on paper or in an unprotected file

25.7 Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

25.8 Passwords must contain a minimum of six characters and be difficult to guess

25.9 User ID and passwords for staff and pupils who have left the School are immediately removed from the system

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

26 Password Security

26.1 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, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

26.2 All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

26.3 Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

26.4 Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Virtual Learning Environment, 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.

27 Personal or Sensitive Information

27.1 Protecting Personal, Sensitive, Confidential and Classified Information

27.1.1 Ensure that any School information accessed from your own PC or removable media equipment is kept secure

27.1.2 Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

27.1.3 Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

27.1.4 Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.

27.1.5 You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its

intended restricted audience

27.1.6 Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

27.1.7 Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

27.2 Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

27.2.1 Ensure removable media is purchased with encryption

27.2.2 Store all removable media securely

27.2.3 Securely dispose of removable media that may hold personal data

27.2.4 Encrypt all files containing personal, sensitive, confidential or classified data

27.2.5 Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

27.3 Remote Access

27.3.1 You are responsible for all activity via your remote access facility

27.3.2 Only use equipment with an appropriate level of security for remote access

27.3.3 To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

27.3.4 Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

27.3.5 Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

27.3.6 Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

28 Safe Use of Images

28.1 Taking of Images and Film

28.1.1 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.

28.1.2 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

28.1.3 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteachers, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

29 Consent of Adults Who Work at the School

29.1 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

30 Publishing Pupil's Images and Work

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

- on the school web site
- on the school's Virtual Learning Environment
- 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 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)

30.2 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.

30.3 Parents may withdraw permission, in writing, at any time.

30.4 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.

31. Storage of Images

31.1 Images/ films of children are stored on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteachers.

31.2 Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Virtual Learning Environment

32 Video Conferencing

32.1 Permission is sought from parents if their children are involved in video conferences

32.2 All pupils are supervised by a member of staff when video conferencing

32.3 The school keeps a record of video conferences, including date, time and participants.

32.4 Approval from the Headteachers is sought prior to all video conferences within school

32.5 No part of any video conference is recorded in any medium without the written consent of those taking part

33 Portable & Mobile ICT Equipment

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

33.2 All activities carried out on School systems and hardware will be monitored in accordance with the general policy

33.3 Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

33.4 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 your car before starting your journey

33.5 Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

33.6 Ensure portable and mobile ICT equipment is made available as necessary for anti- virus updates and software installations, patches or upgrades

33.7 The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

33.8 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

33.9 Portable equipment must be transported in its protective case if supplied

34 Mobile Technologies

34.1 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, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. 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.

35 Personal Mobile Devices (including phones)

35.1 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 using their personal device

35.2 Pupils are not allowed to bring personal mobile devices/phones to

school.

35.3 The school is not responsible for the loss, damage or theft of any personal mobile device

35.4 The sending of inappropriate text messages between any member of the school community is not allowed

35.5 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

35.6 Students and staff should not access social networking sites during school hours from the school premises and should not at any time make comments regarding the school on such sites. Any comments found regarding the school will be removed.

36 School Provided Mobile Devices (including phones)

36.1 The sending of inappropriate text messages between any member of the school community is not allowed

36.2 Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

36.3 Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

36.4 Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

37 Servers

37.1 Always keep servers in a locked and secure environment

38 Mobile Phones

38.1 You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)

38.2 Report the loss or theft of any school mobile phone equipment immediately

38.3 The school remains responsible for all call costs until the phone is reported lost or stolen

38.4 You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it

38.5 School SIM cards must only be used in school provided mobile phones

38.6 All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

38.7 You must not send text messages to premium rate services

39 Reviewing this Policy

39.1 There will be an on-going opportunity for staff to discuss with the Headteachers any issue of eSafety that concerns them

39.2 The policy will be amended if new technologies are adopted

This policy will be reviewed every one – two years or earlier if necessary.

Date: February 2024

Date of review: February 2026