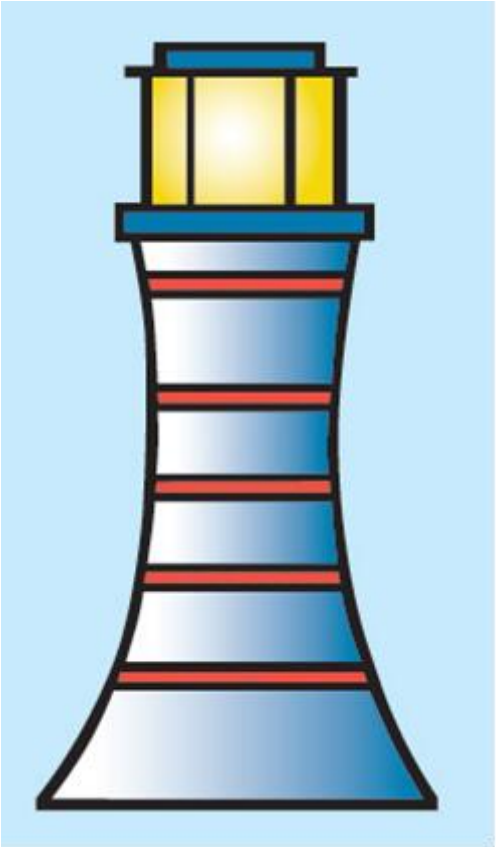
Austhorpe Primary School



ONLINE SAFETY POLICY

Reviewed date: September 2020

Section: Contents: Page:

Appendixes

1. Mission Statement

At Austhorpe Primary School, children are at the centre of everything we do.
We provide a happy, safe and stimulating environment where children are inspired to reach their full potential.
We endeavour to meet the needs of all individuals.
Having high expectations of achievements and behavior, the school team are determined to make a difference.

2. Introduction

2.1. The school makes widespread use of modern technology in the belief and understanding that it can develop and enhance all aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

2.2. The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT.

2.3. This policy

- **applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.**
- **forms part of the school's ICT subject policy and ICT acceptable use policy.**
- **relates to other school policies including, child protection, behaviour and bullying.**
- **also relates to the Leeds Learning Network Internet Access Policy & Email Code of Practice.**
- **has been developed with reference to advice from St Theresa's Catholic Primary School, Education Leeds, the Leeds Learning Network, Becta, Kent County Council and Government guidelines.**
- **often refers to the internet due to this being the major concern. However, it should be noted that there are other aspects of e-safety that need consideration.**

2.4. It is difficult to consider every eventuality within this policy due to the nature of rapid technological change within short timescales.

3. Acknowledgements

We wish to acknowledge the following for their help, advice and permission to use extracts from their documentation:

- **Leeds City Council**
- **Kent County Council**
- **Becta - the British Educational Communications and Technology Agency**
- **St Theresa's Catholic Primary School, Leeds**
- **Children's Services, Children Leeds**

4. Onine Safety

4.1. The increased use of technology at work and at home exposes people to a number of risks and dangers. In its simplest form online safety is about ensuring people use electronic technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

4.2. The Internet is fantastic for information and great for communication, but we all need to know how to use it safely. The children are likely to have internet access in more than one place, so it is important to equip them with the skills to handle this technology safely.

4.3. Online safety is also about protecting the hardware and software we use from

attack illegal	**by unscrupulous people, who may wish to cause disruption or commit acts.**

4.4. Online safety is also about protecting electronic data, our private, personal data and that of other people.

5. Responsibilities

5.1. The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990 (Revised).

5.2. Everyone who uses ICT connected with the school has a responsibility to have a regard for e-safety.

5.3. The Government has placed a responsibility on the Governors and Management of the school to ensure that all employees and pupils are aware

of e-safety concerns and procedures, and that they receive training to raise their awareness of the issues involved.

5.4. The teaching staff have a responsibility, as part of the statutory requirements of the curriculum, to teach e-safety.

5.5. Although the ultimate responsibility lies with the Governing Body and the Headteacher, the school will nominate

- **an Online Safety Coordinator**
- **a Governor with responsibility for online safety issues**
- **a member of the senior management team to deal with online safety issues and online safety complaints in particular**

5.6. The Online Safety Coordinator will

- **oversee the development of this policy**
- **oversee the implementation of this policy**
- **advise the school management on online safety issues**
- **advise staff on online safety teaching and learning resources**
- **be a point of contact for anyone connected with the school who has questions or concerns about online safety issues**
- **be available to deal with general issues of e-safety that are not specific complaints concerning individuals (for example: informing YHGFL of an inappropriate website or a security issue)**
- **be available to deal with minor infringements of the e-safety policy and rules, including accidental infringements**
- **pass on to a nominated senior manager or Headteacher any complaint or evidence received concerning individual pupils or staff misuse of ICT**

5.7. The Headteacher is the school's official administrator for the Yorkshire and

Humber Grid for Learning. However, they may delegate part of this responsibility
to other members of staff.

5.8. Staff who manage the filtering systems or monitor ICT use will be supervised by a
member of the senior management team and work to clear procedures for reporting issues, testing filtering restrictions and checking security systems.

6. Teaching and learning

6.1. Why the Internet and Digital Communications are Important

6.1.1. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

6.1.2. Internet use is a part of the statutory curriculum and a necessary tool for
staff and pupils.

6.2. Internet Use Will Enhance Children's Learning

6.2.1. The school Internet access will be specifically tailored for pupil use and will
include filtering appropriate to the age of pupils.

6.2.2. Pupils will be taught what Internet use is acceptable and what is not and
given clear objectives for Internet use.

6.2.3. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

6.2.4. Pupils will be shown how to publish and present information to a wider
audience.

6.3. Pupils Will be Taught How to Evaluate Internet Content

6.3.1. The school aims to ensure that the use of Internet derived materials by pupils complies with copyright law.

6.3.2. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

6.3.3. Pupils will be taught how to report unpleasant Internet content e.g. to an adult, or using the CEOP Report Abuse icon.

7. Equal Opportunities

The school believes that it is essential that opportunities are provided for everyone to access ICT, regardless of gender, race, religion, culture, ethnic group, sexual

8. Special Needs

8.1. ICT can be a positive tool for children with Special Educational Needs. Access to the Internet is therefore a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas and research independently.

8.2. The school will endeavour to ensure that children with Special Educational Needs are made aware of the risks and dangers of using ICT, within their understanding and abilities. The ICT Coordinator will make appropriate resources available to facilitate this.

9. Managing School Network Access

9.1. The school will maintain two network systems under the control of two separate file servers

- **admin (school administration network)**
- **curriculum**

9.2. The Headteacher will nominate a senior member of staff to oversee the use of the

admin network.
9.3. The ICT Coordinator will have responsibility for the administration of the curriculum network.
9.4. Both servers / networks will be protected by Sophos antivirus software, provided through Yorkshire and Humber Grid for Learning, which will be updated
automatically.
9.5. School ICT systems security will be regularly reviewed.
9.6. Security strategies will be implemented according to guidance from Leeds City
Council, Yorkshire and Humber Grid for Learning and Temple Newsam Learning
Partnership.
9.7. Full access to the admin network will be restricted to senior management and
office staff. Other employees may be allowed limited access to this network for
specific tasks, at the discretion of the Headteacher.
9.7.1. Levels of access to the admin network will be enforced through unique usernames and passwords.
9.7.2. The admin network will be the only network to contain the full details of all
employees and pupils. SIMs etc.

9.8.	**All staff and pupils of the school will be allowed access to the curriculum network.**

9.8.1. Staff will have their own username and unique password in order to use the curriculum network. They will be allocated their own file space and have access to a shared "staff only" area of the network, which the pupils will not be able to access. Staff will also be able to access all pupil folders.
9.8.2. Pupil access will be arranged at different levels appropriate to the age of the
children, through a structured menu system.
9.8.3. All pupils from F2 to Y6 will be allocated their own username and file space.
They will also have access to a "shared area" containing general resources.
9.8.4. Children will not be allowed access to computer equipment at playtimes and

lunchtimes unless a member of staff is present in the room.
9.8.5. Children will not be allowed to work in the ICT Suite without staff supervision.
9.8.6. Parents, visitors, guests and supply staff may be granted restricted access
to the curriculum network, with permission from the Headteacher or ICT Coordinator, through the use of special usernames and passwords.

9.9.	**Contracted I.T. technicians may be given full access to either network, at the discretion of the Headteacher.**

9.10. Only the ICT Coordinator, computer technicians, or other persons nominated by
the Headteacher, may install software on any school workstation or server.
10. Managing Internet Access
10.1. The Internet Service Provider for the school will be RM Education.
10.2. Statutory UK ISP monitoring laws insist that RM Eduation record all Internet
usage and e-mail.
10.3. RM Education will inform the Headteacher if they suspect any misuse of online
services.
10.4. The Headteacher will be the nominated administrator for the school's RM
Education services.
10.4.1. The Headteacher and IT Technician have access to a special RM Education
account that allows the administrator to use RM Education online services with all the restrictions and filters turned off.
10.4.2. According to RM Education regulations, the Headteacher and Chair of the
Governing Body are ultimately responsible for the proper allocation and use of this account.
10.4.3. The Headteacher must be the only person who can give permission to use
this account.
10.4.4. A digital record must be kept of any use of this account.

10.5.	**Staff must adhere to the school's "Code of Conduct for the Acceptable Use of ICT - Staff" when accessing the internet.**

10.6. Staff are not allowed to access the internet other than through the RM Education whilst on the school premises.
10.7. All children will have their own PurpleMash user account with a unique username and password. Children will be able to access safe, managed e-mails
through this service.
10.8. There must be a member of staff present in the room when pupils are accessing the Internet or using e-mail.
10.9. Foundation and key stage 1 pupils must be closely supervised by an adult
when accessing materials using the Internet.
10.10. Pupils must adhere to the school's "Code of Conduct for the Acceptable Use of
ICT – pupils" and "Rules for Responsible Internet Use" when accessing the internet.
10.11. Pupils are not allowed to access the internet other than through the RM
Education whilst on the school premises.
11. Managing Access to E-mail

11. 1.	**Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.**

11. 2.	**Teachers should consider how e-mail from pupils to external bodies is to be presented and controlled before allowing it.**

11.3. The forwarding of chain letters or anonymous mail is not permitted.

11. 4.	**In-coming and outgoing email will be regarded as public and will be monitored by RM Education.**

11.5. Staff will have access to e-mail through their Office 365 account.
11.5.1. Staff e-mail accounts are for school related use and can only be used for
private purposes at the discretion of the Headteacher. No private business activities of any nature may be undertaken. All school related e-mails should be sent using Office 365 accounts.
11.5.2. Staff may only access a private or home e-mail account on school premises
outside normal timetabled hours. However, this should be kept to a minimum and staff should follow the school's "Code of Conduct for the

Acceptable Use of ICT - Staff" when doing so. The Headteacher reserves the right to withdraw this arrangement at any time.
11.5.3. Staff should inform the Headteacher if they receive offensive e-mail.
11.6. Pupils must adhere to the school's "Code of Conduct for the Acceptable Use of
ICT – pupils" and "Rules for Responsible Internet Use" when using e-mail.
11.6.1. Pupils are not allowed to access a private or home e-mail account on school premises.
11.6.2. Pupils must immediately tell a teacher if they receive offensive e-mail.
12. Managing Other Technologies
12.1. Published Content and the School Website or Learning Platform
12.1.1. Staff or pupil personal contact information will not generally be published.
The contact details given online should be the school office or Headteacher.
12.1.2. The Headteacher will take overall editorial responsibility and ensure that
content is accurate and appropriate.
12.1.3. All material published on the school website must be the author's own
work. If material from other sources is included credit should be given to the original author, stating clearly the source of such work and must not break copyright laws.
12.1.4. Work belonging to a pupil can only be published with the permission of the
pupil and their parents / carers.
12.1.5. Photographs that include pupils will be selected carefully so that individual
pupils cannot be identified or their image misused. Consideration should be given to using a group photograph rather than full-face photos of individual children.
12.1.6. Pupils 'full' names will not be used anywhere on the school website, particularly in association with photographs.
12.1.7. Pupil image file names will not refer to the pupil by name.
12.1.8. Written permission from parents or carers will be obtained before photographs of individual pupils are published on the school website.
12.1.9. Parents should be clearly informed of the school policy on image taking
and publishing, both on school and independent electronic repositories

12.2. Social Networking and Personal Publishing

12.2.1. Pupils will not be allowed to access social networking sites, instant messaging sites or chat rooms, on school premises, with the exception of safely managed Purple Mash accounts.

12.2.2. Pupils will not be allowed access to video websites filtered by RM Educaiton on school premises.

12.2.3. Newsgroups may not be used by pupils unless specifically approved by their teacher.

12.2.4. Pupils are taught never to give out personal details of any kind which may identify them, their friends or their location.

12.2.5. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Ideally pupils should use only moderated, child friendly, social networking sites. Pupils will be advised to use nicknames and avatars when using such social networking sites.

12.2.6. Members of staff must not access social networking sites from school network.

12.2.7. It is not permitted for staff to allow pupils to name them in any "friends" or contacts list on a social networking site, unless they are actually a relation of the pupil.

12.3. Managing Videoconferencing and Webcam Use

12.3.1. Videoconferencing should use Joint Academic Network (JANET), accessed via RM Education to ensure quality of service and security.

12.3.2. Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

12.3.3. Videoconferencing and webcam use must be appropriately supervised for the pupils' age.

12.4. Mobile Phones

12.4.1. All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

12.4.2. Pupils are not allowed to use mobile phones, tablets or technologies built

in to a mobile phone, on school premises or during school activities off-site unless specially commissioned hardware is owned by the school.
12.4.3. Staff should not use their own communication technologies to capture
photographs of pupils. (see paragraph 12.5.4 below)
12.5. Digital Cameras including iPads
12.5.1. It should be noted that there are risks to allowing the capturing digital images on the school premises. It is easy for anyone to manipulate digital images, using modern software, and put them to inappropriate uses.
For example: Pupils using images to bully other pupils or staff;
Pupils manipulating an image and publishing a
compromising version on the internet.
12.5.2. It should be noted that digital cameras can be used to spread computer
viruses, in a similar way to memory sticks.
12.5.3. Staff and pupils may use digital cameras belonging to the school, as part of
the curriculum, to provide evidence or as a record of work.
12.5.4. Staff should not capture images of pupils on personal digital cameras. Staff who do so would put themselves at risk should a pupil or parent bring a complaint against them. It would be harder to prove that the images were taken for school purposes, especially if the images were taken home on the camera.
12.5.5. Digital copies of images of staff or pupils must not be e-mailed or given to
someone outside the school premises without permission from the Headteacher.
12.5.6. Images taken with a school digital camera should be kept in the cameras
memory, or on the memory card, for as short a time as possible and then be deleted. Images should not be stored on a camera for long periods and certainly not indefinitely.
12.5.7. Pupils should not be allowed to use personal digital cameras on the school
premises unless permission is granted by the Headteacher for a specific use, and only then under close supervision and with great care.
12.5.8. If sanctioned by the Headteacher, pupils will be allowed to use personal
digital cameras on a school activity off the premises. Close supervision would be essential and limits should be explained to the pupils.

12.5.9. **Staff should note that some games machines including the Sony Playstation, Microsoft Xbox, Nintendo DSi and other hand-held consoles, have a built in webcam. Such devices may also be capable of instant messaging when in close proximity to others, without using the internet. It is not advisable to allow their use in school. Staff should get permission from the Headteacher before allowing the use of such devices in school. (See also paragraph 12.9.3)**

12.6. Laptops

12.6.1. When on the school premises, pupils may only use laptops provided by the

school. They are not allowed to bring personal laptops on to school premises.

12.6.2. Staff provided with a laptop purchased by the school can only use it for

private purposes at the discretion of the Headteacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the ICT Coordinator.

12.6.3. Laptops belonging to the school must have active antivirus software installed and be password protected.

school. Staff should get permission from the Headteacher before allowing the use of such devices in school. (See also paragraph 12.5.9)

13. Authorising Access

13.1. The final decision as to who can be granted access to school ICT equipment and facilities will rest with the Headteacher.

13.1.1. A nominated member of the senior management will be responsible for supervising access to the admin network.

13.1.2. The ICT Coordinator will be responsible for supervising access to the curriculum network and classroom ICT equipment.

13.1.3. The Headteacher is responsible for supervising access permissions to the RM Education but may delegate some of this responsibility to other members of staff.

13.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

13.3. All staff must read and sign the "Code of Conduct for the Acceptable Use of ICT - Staff" before using any school ICT resource. This is to be renewed at the start of each new school year (normally in September).

13.4. Temporary staff and supply staff regularly used by the school will be granted access to the curriculum network, through being allocated their own username and password, and will read and sign the "Code of Conduct for the Acceptable Use of ICT - Staff" before using any school ICT resource. This is to be renewed on an annual basis, at least.

13.5. Parents will be asked to sign and return a consent form concerning their child's use of the RM Education.

13.6. Visitors and any person not directly employed by the school, needing to use ICT

resources, will be asked to sign a "Code of Conduct for the Acceptable Use of ICT Resources – Visitors" form before being allowed to access the curriculum network or the internet.

14. Protecting Personal Data

14.1.	**Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.**

14.2.	**Every member of staff must take all reasonable steps to securely protect all data concerning pupils and others.**

14.3.	**All school computer systems must be password and virus protected, including school equipment used at home by staff.**

14.4. Any data taken off the school premises should be kept to a minimum and if no longer required, deleted or destroyed in an appropriate manner, or returned to school for destruction.

14.5.	**All printed copies of personal data must be shredded before disposal as waste material.**

14.6. There is a security / data protection risk when computer equipment is taken out of use and disposed of. Hard disks from computers should be adequately erased before machines are recycled, especially if being taken off the premises. Hard disks that have contained sensitive data (such as those from the admin network) should be destroyed rather than recycled.

14.7.	**Staff must take all reasonable care when using, storing and transporting memory sticks, CDs or DVDs containing school data.**

14.8. School memory sticks containing pupil details (e.g. assessment or reports) will be password encrypted, otherwise data should not be transported.

14.9. Memory sticks provided by school must not be used for private purposes and remain open to scrutiny by senior management, contracted technicians and the ICT Coordinator.

14.10. Anyone transferring personal data from school sources to their own personal computer or memory stick is personally liable for the security of the data and for any legal consequences.

14.11. When working with personal or confidential data computer screens should be positioned where they are not easily visible from outside the immediate work area or by an unauthorized person.

15. Assessing Risks

15.1. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school, Children Leeds, RM Education and Leeds City Council do not accept liability for any material accessed, or any consequences of ICT or Internet access, either on school premises or through the RM Education

15.2. The school will develop procedures to audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

15.3. The final decision when assessing risks will rest with the Headteacher.

16. Handling Online Safety Complaints

16.1.	**Complaints of ICT / Internet misuse will be dealt with by a senior member of staff, who will decide if any sanctions are to be imposed.**

16.2.	**Any complaint about staff misuse must be referred to the Headteacher, who will decide if any sanctions are to be imposed.**

16.3.	**Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.**

16.4. The Headteacher will arrange contact / discussions with Children Leeds and the Police Authority to establish clear procedures for handling potentially illegal issues.

16.5. Any complaint about illegal misuse must be referred to the Headteacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Children Leeds.

16.6.	**All employees, pupils and parents will be informed of the complaints procedure.**

16.7.	**All employees, pupils and parents will be informed of the consequences of misusing ICT or the Internet.**

16.8. Sanctions for minor incidents could include

- **informing parents or carers, when a pupil is involved**
- **receiving a verbal warning, of which a record is kept**
- **receiving a formal written warning**
- **having network or Rm Education access denied for a specified period**

16.9.	**Sanctions for other incidents, especially after warnings have been given, could include**
•	**informing parents or carers, when a pupil is involved**

- **having network or Rm Education access permanently revoked**
- **formal disciplinary action being taken against an employee**

16.10. Staff should note that copies of illegal material they find should not be sent / forwarded to anyone else, even as evidence, as this could also be seen an committing an illegal act.

16.10.1. Do not e-mail copies of illegal material to the Headteacher, Online Safety Coordinator, Child Protection Coordinator or the RM Eudcation Service Desk, as receiving such material could also be seen as the committing of an illegal act on their part.

17. Communicating Policy

17.1. Introducing the Online Safety Policy to Pupils

17.1.1. Online Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

17.1.2.	**Pupils will be informed that network and Internet use will be monitored and appropriately followed up**

17.1.3. A programme of training in e-Safety will be developed, possibly based on

the materials from CEOP.

17.1.4. E-Safety training will be embedded within the ICT scheme of work and the
Personal Social and Health Education (PSHE) curriculum.

17.2. Staff and the Online Safety Policy

17.2.1.	**All staff will be given the School Online Safety Policy and its importance explained.**

17.2.2. Appropriate training will be arranged for all staff.

17.2.3.	**All temporary staff and supply staff used regularly by the school will be given the School Online Safety Policy and its importance explained.**

17.2.4. Every member of staff, whether permanent, temporary or supply staff regularly used by the school, must be informed that network and Internet traffic will be monitored and can be traced to the individual user.

17.3. Enlisting Parents' and Carers' Support

17.3.1.	**Parents and carers attention will be drawn to the School Online Safety**
Policy in website.	**newsletters, the school brochure and on the school**

17.3.2. The school will maintain a list of e-safety resources for parents / carers.

17.3.3.	**Links to useful internet websites, with advise for parents, will be built in to the school website**

17.4. Visitors and the Online Safety Policy

17.4.1. Not all visitors will need to use school ICT but those which do will need to
be informed that the school does have an Online Safety policy and they should be given the opportunity to read it, if the Headteacher thinks that it would be appropriate.

17.4.2. Visitors using school computer technology must be informed that network and Internet traffic will be monitored and can be traced to the individual user.

18. Policy Approval and Review (* staff should alter the appropriate dates as necessary)

18.1. The first draft of this policy was discussed by the teaching and learning committee during November 2009. Amendments were suggested and version 2
circulated.

18.2. The second draft was discussed by the staff during December 2009. Amendments were suggested.
18.3. This final version (V2) was approved by the Governing Body in January 2010.
18.4. V2 was reviewed December 2012. The next version (V3) was then produced.
18.5. It was reviewed in July 2015. The next version (V4) was then produced.
18.6. It was reviewed in line with new advice and guidance in March 2017, including
changing the policy name from "E-Safety Policy" to "Online Safety Policy". The
current version (V5) was produced.
18.7. A full copy of this policy will be given to:
- **each member of the teaching staff**
- **each member of the administrative staff**
- **each member of the support staff**
- **supply staff regularly used by the school**

18.8. A copy will also be available
- **to other interested parties, by request to the Headteacher or Computing Coordinator**
- **as a .doc file in the staff section of the curriculum network**

19. Nominated Persons
The following persons are nominated until further notice:
19.1. The nominated member of the senior management team with responsibility for
online safety is Miss. A Lightfoot (Headteacher).
19.2. The nominated Online Safety Coordinator is Mr. A. Morley.
19.3. The nominated Governor with responsibility for online safety is Mrs. Julie
Webster (Vice Chair and ICT Governor).
END