Amesbury Internet Safety Policy

Contents

Version Control

As part of the maintenance involved in ensuring the Internet safety policy is updated, revisions will be made to the document annually.

Title	Amesbury Online safety policy
Version	1.9
Date	22/05/2020
Author, Internet safety officer	Mr Tony Sharps
Approved by Headmistress	Sheina Wright
Approved by Governors Safeguarding Committee	Matthew Bryan
Approved by Governing Body (Chair)	Mr Tarquin Henderson
Next Review Date	April 2021

Modification History			
Version	Date	Description	Revision Author
0.1	07/08/14	Draft Policy	Tony Sharps
02	07/11/14	Second Draft	Tony Sharps
03	20/11/14	Final Document for presentation	Tony Sharps
04	21/04/16	2016 review	Tony Sharps
05	05/05/17	2017 review	Tony Sharps
06	25/05/18	2018 review	Tony Sharps
07	25/09/18	2018 Revision	Tony Sharps
08	13/05/2020	2020 Revision	Tony Sharps
09	22/05/2020	Name change to Online Safety policy. Minor tweak to reflect new Matthew Bryan	Tony Sharps

		taking over as SG governor	

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Amesbury with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Amesbury.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community

can be summarised as follows:

Content

- Exposure to inappropriate content. Including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites and sites promoting extremist views.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming (CSE, Radicalisation etc.)
- Online-bullying in all forms.
- Identity theft, including passwords.

Conduct

- Aggressive behaviours (bullying, trolling)
- Privacy issues, including disclosure of personal information.
- Digital tattoo and online reputation.

- Health and well-being (amount of time spent online (internet or gaming)).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of the Amesbury community (including staff, students / pupils, governors, volunteers, parents / carers, visitors and community users) who have access to and are users of the school's ICT systems, both on and off the school premises.

Any incidents which result in a breach of this policy will be dealt with in accordance with the guidelines set out in the staff disciplinary policy or pupil behaviour and anti-bullying policy. Should we become aware, we will inform parents / carers of any inappropriate online behaviour that takes place outside of school.

Key Roles

Designated Safeguarding lead	Michael Armitage	Deputy Headmaster
Designated Safeguarding Lead EYFS	Jackie Collyer	Head of EYFS
Deputy Designated Safeguarding Lead	James Balcombe	Year 4 Teacher
Internet Safety Officer	Tony Sharps	Head of IT
Chair of Governors	Tarquin Henderson	
Safeguarding (prevent) Governor	Matthew Bryan	
Head of PSHEE	Caroline Munday	
Head of Computing	Patricia Risley	

Communication

The policy is communicated to school stakeholders in the following ways:

- Via the school website
- New Parents Handbook, Staff Handbook, School computer network
- Induction packs for new staff
- Safeguarding Induction Training for New Staff
- On an ad hoc basis to new families joining the school during the year.
- Acceptable Use Agreements are discussed with all pupils at the start of each year
- Regular Internet Safety workshops are provided for parents
- Staff are given Internet Safety updates at least annually as part of the INSET Program

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The DSL acts as the first point of contact for any incident, DDSL in their absence.
- Any suspected online risk or infringement is reported to the Head of IT that day.
- Any concern about staff misuse is always referred directly to the Head, unless the concern is about the Head in which case the compliant is referred to the Chair of Governors.
- Should the incident involve nude selfies or sexting, the Sexting in schools and Colleges guide will be used to determine the best course of action. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf
- Data breach guidelines and reporting forms are available in the staff handbook
- Content filters automatically report the use any suspicious or concerning search terminology directly to the DSL.
- Online safety incidents are recorded in the school's CPOMS system.

Review and Monitoring

The Internet safety policy is referenced from within other school policies: Staff Code of Conduct, Pupil behaviour and anti-bullying, Taking using and storing images of children,

- The school has an Internet safety Officer who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online safety policy has been written by the school Internet safety officer and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by the Governors safeguarding sub-committee and Governing Body.
- Amendments to the policy will be disseminated to all members of staff

Education and Curriculum

Online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas where applicable. This covers a range of skills and behaviours appropriate to pupil age and experience;
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- Recognises and promotes UK Safer Internet Day.
- Broadens the message by inviting external speakers in to discuss Internet Safety.
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- Makes regular training available to staff on online safety issues and the school’s online safety education program as part of the INSET program and twilight training sessions.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school’s Acceptable Use Agreements as part of the employee code of conduct.
- The safeguarding governor receives regular Internet Safety updates as the topic is a recurring agenda item for safeguarding meetings.
- The Internet Safety Officer briefs the full governing body on significant developments or initiatives. e.g The Prevent Duty.

Parent awareness and training

This school:

- Runs a program of parent lectures and workshops exploring aspects of Internet Safety
- Broadens the message by inviting external speakers in to discuss Internet Safety.
- Makes the Internet Safety officer available for parents.

Expected Conduct

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements or Code of Conduct
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school
- Know and understand school policies on the use of mobile and hand held devices including cameras

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils

Parents/Carers

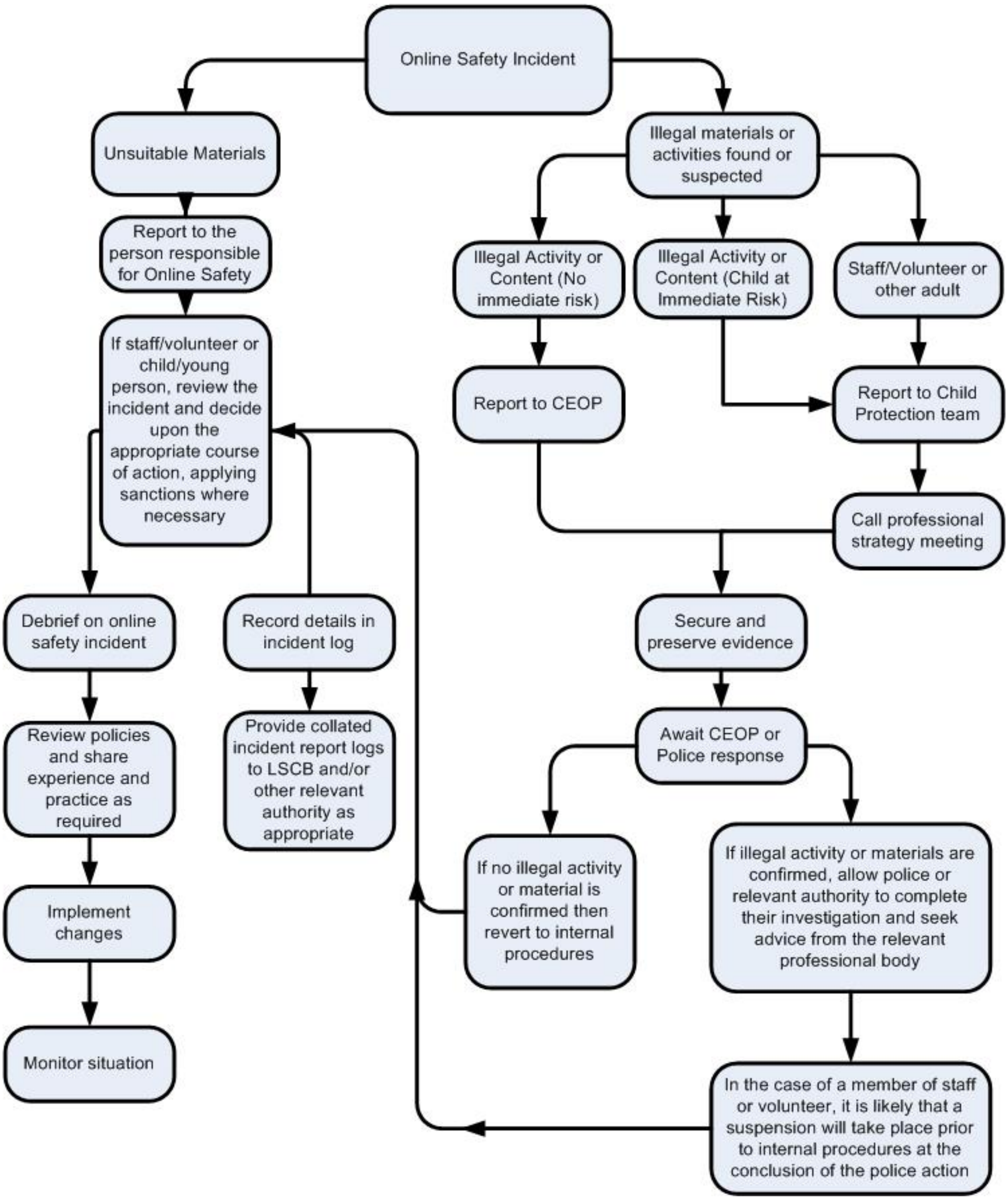
- Understand that use of the Internet is an endemic factor of modern education.
- Provide consent for use of additional technologies such as the issuing of mobile technology (iPads, laptops for learning support).

Incident Management

In this school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Incident Workflow


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;
- Uses web content filtering supplied by LightSpeed Systems. Allowing granular and targeted filtering to all stakeholders when using the School Internet connection or a school mobile device. All Internet activity is logged and traceable. All alterations to filtering are logged and access restricted to members of the IT department
- Enforces Google and Bing SafeSearch. By extension YouTube.
- Places a strong emphasis on teaching discernment and making good judgements whilst online
- Ensures good network health by the use of Sophos Anti-Virus, Cisco firewall, Lightspeed content filters, Microsoft O365 Anti-Spam and regular auditing
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable
- Ensures pupils only publish within an appropriately secure and moderated environment
- Requires staff to preview websites implicitly used within the curriculum before use [where not previously viewed or cached]
- Plan the curriculum context for Internet use to match pupils' ability.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs staff that any failure of the filtering systems is reported promptly to the IT department

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Storage of all data within the school will conform to the UK data protection requirements
- Data stored externally to the school will be housed exclusively in the school's Microsoft Office 365 environment. Use of data stored externally will conform to GDPR regulations.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
- Backups are performed daily to disk storage held securely onsite in a separate physical location to the sever infrastructure. Backups are stored on magnetic media weekly and stored securely in a fire proof safe in a separate physical location to the server infrastructure.

Ensuring the network is used safely

This school:

- Ensures staff read the Online Safety Policy and agree to abide by the associated Staff Code of Conduct.
- Prep School pupils have their own unique username and password which gives them access to the Internet and other services;
- Pre-prep pupils have a generic login, use of which is controlled
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working
- Requires users to lock their computer if they are leaving it unattended
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any laptop or iPad loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Our wireless network has been secured to industry standard Enterprise security level
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;
- Uses the following security technologies: Sophos Anti-Virus, Cisco firewall, Lightspeed content filters and MDM, Microsoft O365 Anti-Spam

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to change their network and MIS passwords every 180 days.

E-mail

This school:

- Does not publish personal e-mail addresses of pupils on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.

- Knows that SPAM, phishing and virus attachments can make e-mails dangerous. We use enterprise class technologies to identify and nullify any threats alongside end user education on what to do should they be in receipt of unsolicited e-mail.

Pupils

- Pupils from year 1 are issued with e-mail. In Year 1-4 e-mail is in a walled garden environment called Purple Mash. Pupils in years 5-8 use e-mail to communicate within the school. E-mail accounts cannot send / receive external e-mail.
- Pupils are taught about the online safety and etiquette of using e-mail both in school and at home.

Staff

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Never use email to transfer staff or pupil personal data.

School website

- The Marketing Department, supported by the Governors marketing committee, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Images used on the school website comply with the regulations as set out in the policy Taking, using and storing images of children.
- The school website complies with ICO guidelines on data protection.

Cloud Environments

This school:

- Exclusively uses Microsoft Office 365 for school data.
- Conducts a PIA for any 3rd party App or service requiring the use of personal data.
- Ensures pupils use only school sanctioned cloud environments.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools’ preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.
- Staff have strict instructions on their social media conduct outlined in the Code of Conduct
- Pupils are exposed to a model internal social network as part of Computing lessons in order to learn acceptable online behaviours.

Data security Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head is the Senior Information Risk Officer (SIRO).
- Information Asset Owners: Finance – Bursar Yvonne Drew, Admissions – Liz Wright, Academic Data – Jackie Bowers.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record
- Staff digital storage areas will be audited annually and staff advised to archive or delete old or infrequently used contents.

- Staff have a secure area of the network for the storage of sensitive documents
- All servers are housed in a secure area and managed by DBS-checked staff.
- We store backup media in a secure fire-proof cabinet. Backups are encrypted.
- We use a secure NAS solution as secondary backup. Backups are encrypted.
- We comply with regulations regarding WEEE by using an approved or recommended disposal company for disposal of all waste electronic equipment. We receive a certificate of secure destruction for any media (Hard Disk Drives) that are disposed.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated technology free areas are situated in the setting, and signs to this effect are displayed demarcating these areas. The areas considered most vulnerable are: EYFS, toilets, bathrooms, boarding and changing areas.
- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils are not permitted to bring mobile phones onto site.
- The School reserves the right to impound any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the Head or DSL
- Where parents or pupils need to contact each other during the school day, they should do so only through the School office. Staff may use their phones during break times. Use outside of break times should be Emergency Only.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- Staff use of mobile technology is governed by the Staff Code of Conduct and Taking, Using and Storing images of Children policies
- In EYFS, staff use of mobile phones and personal devices is prohibited. Devices are stored in a locked cupboard throughout the day.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.

Appendix 1 – Pupil AUP Pre-Prep

Pupil IT Acceptable Use Policy for Early Years and Y1-Y4 Pupils

This is how we stay safe when we use computers:

I will ask my teacher if I want to use a computer or iPad

I will only do things that my teacher or another adult has said I can do

I will take care of the computer and other equipment

I will ask for help from my teacher if I think I have done something wrong

I will tell my teacher if I see something that upsets me on the screen

I know that if I break the rules I might not be allowed to use a computer or iPad

Amesbury Pupil IT
AUP EYFS & Pre-prep

Appendix 2 – Pupil AUP Prep

Pupil IT Acceptable Use Policy for Y5-Y8 Pupils

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

I will keep myself safe:

- I understand that Amesbury will monitor my use of the school systems, devices and digital communications.
- I will keep my username and password safe and secure.
- I will only use the school systems logged on as myself.
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource:

- I understand that Amesbury's systems and devices are primarily intended for educational use. I will not use them for personal or recreational use unless I have permission from a teacher.
- I will not use Amesbury's systems or devices for activities that are inappropriate for my age. Examples would be on-line gaming, internet shopping, file sharing, or accessing inappropriate websites.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the permission of the owner.
- I will be polite when I communicate with others and will appreciate that others may have different opinions to my own.
- I will not take or distribute images of anyone without their permission and must only use the images for school purposes.
- I will help Amesbury to ensure that nobody uses the Internet to bully anyone online. I know that Amesbury takes incidents of bullying very seriously.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Amesbury.

- I will not bring any personal devices into school unless I have permission to do so.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open an email if I am concerned about its validity nor will I open any hyperlinks or attachments, unless I know and trust the person / organisation that sent the email.
- I will not forward e-mails containing jokes or spam.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

I will use the Internet responsibly for research and recreation:

- I should ensure that I have permission to use the original work of others in my own work and will reference the original.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I will use the Internet responsibly for research and recreation:

- I should ensure that I have permission to use the original work of others in my own work and will reference the original.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

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

- I understand that all my actions on the Internet that relate to me being a pupil at Amesbury are covered by this Acceptable Use Policy agreement. This is the case whether the actions take place in school or out of school. (Examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. Amesbury Pupil IT AUP Prep school.pd