Online Safety Policy

Contents

Version Control 2
Key Roles 3
Introduction 3
Scope 3
Communication 4
Review and monitoring 4
Handling Incidents 5
  Incident Workflow 6
Education 7
  Online Safety Curriculum 7
  Staff and Governor Training 8
  Parent Awareness and Training 8
Expected Conduct 8
  All Users 8
  Staff, Volunteers and Contractors 8
  Pupils 9
  Parents / Carers 9
Internet and Cloud Services 9
  Internet Access 9
  Cloud Services 9
  Website/Social Media Channels 10
E-mail 11
Infrastructure 11
  Network 11
  Password Policy 12
Data Protection 12
Equipment 12
  BYOD 13
  School Owned 13
Appendix 1. Pupil AUPs 14

Version Control

The Online Safety Policy will be reviewed annually

Title	Online Safety Policy
Version	2.0
Date	22/05/2021
Author	Tony Sharps
Approved by Head	Jonathan Whybrow
Approved by Governors Safeguarding Committee	Matthew Bryan
Approved by Governing Body (Chair)	Mr Tarquin Henderson
Next Review Date	April 2022

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 Matthew Bryan taking over as SG governor	Tony Sharps
2.0	22/05/2021	Re-write	Tony Sharps

Key Roles

Designated Safeguarding lead	Michael Armitage	Deputy Headmaster
Deputy Designated Safeguarding Lead	Nick Randall	Teacher, Year 5 tutor
Internet Safety Officer	Tony Sharps	Head of IT
Chair of Governors	Tarquin Henderson	
Safeguarding (prevent) Governor	Matthew Bryan	
Head of Computing	Patricia Risley	

Introduction

The purpose of this policy is to:

- Set out expectations of all members of the school community with respect to the attitudes, behaviours and use of digital technologies, including when devices are offline.
- Safeguard and protect the children and staff of Amesbury.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- 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 misdemeanours and clear structures to follow where there are doubts or concerns.
- 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.

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 our digital technology whether on-site or remotely, at any time.

Communication

This policy is communicated to 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

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

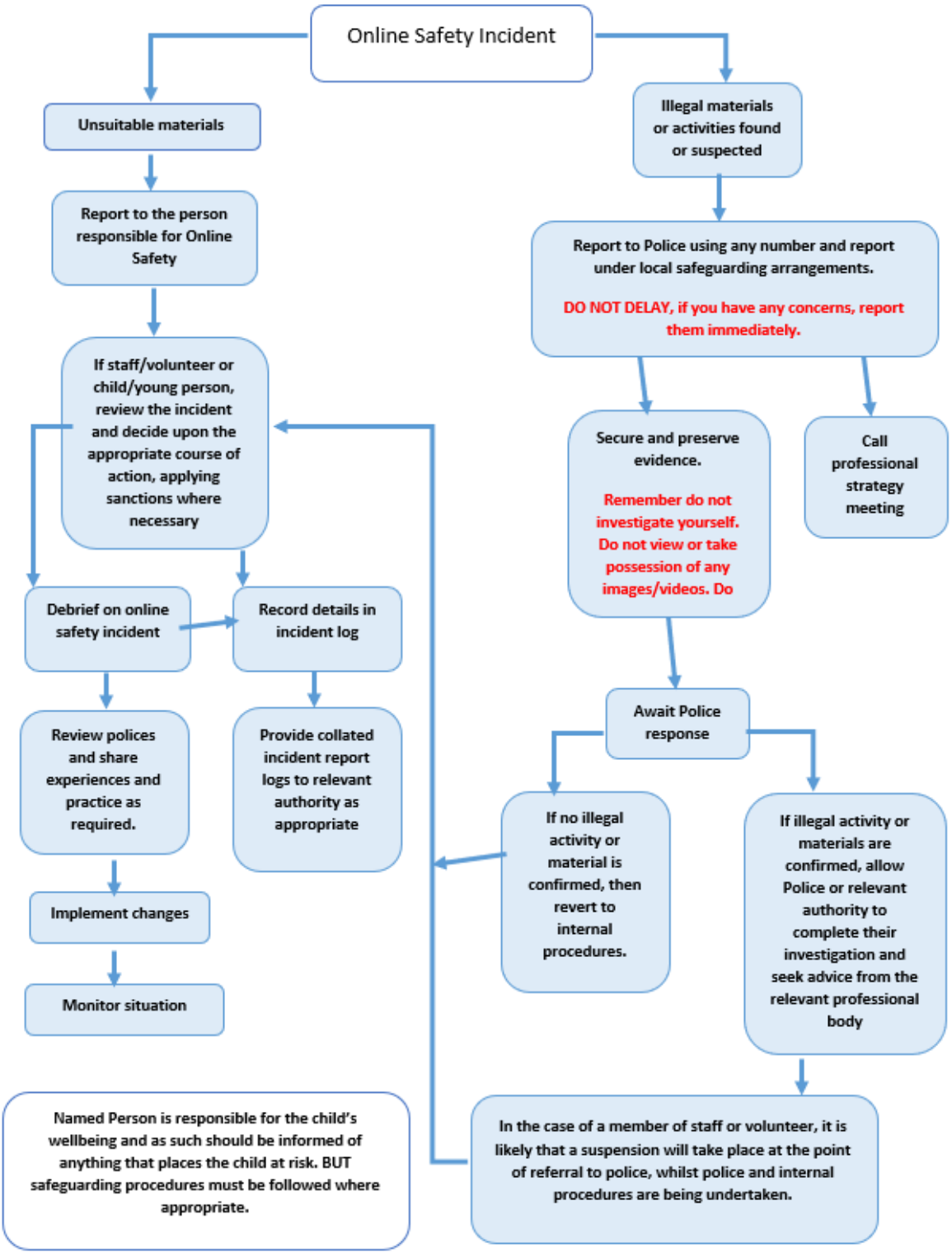
Handling Incidents

It is vital that all stakeholders recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern.

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.

- The school takes all reasonable precautions to ensure online safety.
- 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, Channel, Police, IWF) in dealing with online safety issues.
- 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 complaint is referred to the Chair of Governors. A staff whistleblowing policy is available in the Staff Handbook.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- Should the incident involve nude selfies or sexting, the guide available at the following link will be used. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947545/UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_settings_V2.pdf
- It is important that everyone understands that upskirting is a criminal offence.
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.
- Data breach guidelines and reporting forms are available in the staff handbook.
- Content filters automatically report the use of any suspicious or concerning search terminology directly to the DSL.
- Online safety incidents are recorded in the school's CPOMS system.

Incident Workflow



Education

Online Safety Curriculum

This school:

- Has a clear, progressive PSHE/RSE program. Including being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.
- Has a clear, progressive Computing program which covers the principles of online safety at all key stages, including how to use technology safely.
- 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) and associated lessons.
- 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. The topic is a recurring agenda item for both safeguarding and digital committee 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's digital 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

- Understand that Online-Safety is a core part of safeguarding.
- Carefully supervise and guide pupils when engaging in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best practise at all times including password security and phishing strategies.
- Encourage pupils to follow their acceptable use policy whether they are engaged in remote work or in school.

- Take a zero-tolerance approach to bullying.
- Model safe, responsible and professional behaviours in their own use of technology. In accordance with the Staff Code of Conduct.
- Makes clear that staff are responsible for ensuring that any device loaned to them by the school is used primarily to support their professional responsibilities.
- Staff 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 have strict instructions on their social media conduct outlined in the Code of Conduct.

Pupils

- Read understand and adhere to the Acceptable Use policy.
- Treat home learning the same way as learning in school.

Parents / Carers

- Consult with the school if there are any concerns about their children's or other children's use of technology.
- Promote online safety.
- Support remote learning by ensuring appropriate standards of dress and location whilst at home.

Internet and Cloud Services

Internet Access

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 (inc YouTube) and Bing SafeSearch.
- Places a strong emphasis on teaching discernment and making good judgements whilst online.
- 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.
- 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.

Cloud Services

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.

Website/Social Media Channels

- The Marketing Department, supported by the Governors marketing committee, takes overall responsibility to ensure that the website/social media 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.

E-mail

This school:

- Does not publish e-mail address of pupils externally.
- 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.
- 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 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.
- 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.

Infrastructure

Network

This School:

- Ensures good network health by the use of Sophos Anti-Virus, Meraki firewall, Lightspeed content filters, Microsoft O365 Anti-Spam and regular auditing.
- Uses individual, audited log-ins.
- 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.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Requires all users to log off when they have finished working .
- Requires users to lock their computer if they are leaving it unattended.
- 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.
- 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.
- Our wireless network has been secured to industry standard WPA/2 Level.

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.

Data Protection

- The Head is the Senior Information Risk Officer (SIRO).
- Information Asset Owners: Finance and HR – Bursar Yvonne Drew, Admissions – Liz Wright, Academic Data – James Guest.
- 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 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 containing data that is disposed.
- 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.
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.
- MIS functions and data access is restricted by role.

Equipment

- 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 and changing areas.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School office.

BYOD

- Pupils are not permitted to bring into school any personal device that can connect to the Internet either by WiFi or the cellular network. E.g. Mobile phone, eBook reader, smart watch.
- Personal devices brought into school by staff members, parents or visitors are at their own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- 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
- 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 used solely for the NHS contact tracing App and must not be used for sending images or files to another device. 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.

School Owned

- Devices issued to staff and pupils remain the property of the school.
- Devices are issued for school work only.
- Devices will be audited at least annually.

Appendix 1. Pupil AUPs

AMESBURY

IT Acceptable Use Policy

(Early Years)

This is how we stay safe when we use school iPads

I will ask an adult if I want to use a school iPad. I will not bring in any tech from home

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

I will take care of the iPads and other equipment

I will ask for help from an adult if I think I have done something wrong

I will tell an adult 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 the school iPads

AMESBURY

IT Acceptable Use Policy (Y1 and Y2)

This is how we stay safe when we use school iPads

I will ask an adult if I want to use a school iPad. I will not bring in any tech from home.

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

I will only use my own login details

I will not change the work of other people

I will be polite when I communicate with other people using the iPads

I will ask the person before I take a photo of them

I will check with an adult before I type any personal information

I will ask for help from an adult if I think I have done something wrong

I will tell an adult if I see something that upsets me on the screen

I will take care of the school iPads and will tell an adult if an iPad is damaged or not working

I know that if I break the rules I might not be allowed to use the school iPads

Date of policy: TS May 2021
Date of Review: May 2022

AMESBURY

IT Acceptable Use Policy (Y3 and Y4)

I understand that I must always use school systems and computers responsibly and safely

I will ask an adult if I want to use a school computer. I will not bring in any tech from home eg a Switch or smart watch

I will only use school systems and computers to do things that my teacher would like

I will not tell anyone my password and will only use school systems and devices logged on as myself

I will respect the work of other people when I work collaboratively; *I will not delete or change anything done by someone else without their agreement*

I will be polite when I communicate with others and know that other people may have different opinions to mine

I will not take photos or share them without the permission of the person in the photo

I will only use websites that my teacher has said I can use

I will check with an adult before I type any personal information

I will ask for help from an adult if I think I have done something wrong

I will tell an adult if I see something that upsets me on the screen

I will take care of the school computers and will tell an adult immediately if a computer is damaged or not working

I know that if I break the rules I might not be allowed to use the school computers

Date of policy: TS May 2021
Date of Review: May 2022

AMESBURY

IT Acceptable Use Policy (Y5-Y8)

I understand that I must use school systems and devices responsibly, 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 know that the only device I can bring into school is my school-issued laptop; I know that no ot internet enabled device is permitted eg phone, tablet or smart watch. *I will only use my schoo device and accounts for school work and will not deface them*

I understand that everything that I do on school systems and devices will be monitored and that everything that I create belongs to the school

I will not tell anyone my password and will only use school systems and devices logged on as myself

I will respect the work of other people when I work collaboratively; *I will not delete or change anything done by someone else without their agreement*

I will be polite when I communicate with others and recognise that other people may have different opinions to mine

I will not take photos or share them without the permission of the person in the photo

I will use the Internet responsibly; *I will reference sources, respect copyright and attempt to verify that information is correct*

I will think before I post personal information online; *I know that it is very difficult to remove information that has been posted on the Internet*

I will report immediately any unpleasant or inappropriate material or messages, or anything that I see on screen that makes me feel uncomfortable

I will not install programs of any type on a school device without permission

I will not attempt to by-pass systems put in place to keep me and the school systems and devices safe

I will report immediately any damage or faults to school systems, devices or software

I understand that all my actions using school systems and devices are covered by this Acceptable Use Policy, no matter whether the actions take place in or out of school

Date of policy: TS May 2021
Date of Review: May 2022