Priors Hall – a learning community

Online Safety and Usage Policy

2021 - 2022

'Ready for Learning, Ready for Life'

Curiosity Kindness Resilience Respect

Adopted September 2021 Reviewed July 2022

Contents Page

1. Online safety and internet usage	1.1 Introduction 1.2 Why is internet use important? 1.3 How does internet use benefit education? 1.4 How can internet use enhance learning 1.5 Good habits 1.6 Dangers to consider
2. Online Safety Audit	
3. Specific Safeguarding Considerations	3.1 Internet Access and Responsibility 3.2 Email and Online Collaboration 3.3 Social Networking 3.4 Cyberbullying 3.5 Filtering and Information System Sharing 3.6 Managing Emerging Technology 3.7 Published Content on the School's Website 3.8 Protecting Personal Data and GDPR 3.9 Assessing Risk 3.10 Handling Online Safety Complaints 3.11 Communication with All Stake Holders
4. Priors Hall Safeguarding Statement	
Appendices	A) Staff and Governor Acceptable Use Agreement B) Children's Acceptable Use Agreement C) Letter to Parents example (KS2) D) Use of Technology in School E) SMART online safety rules

Key Contacts

Headteacher	Tess McQuade tessmcquade@priorshallalc.com
Designated Safeguarding Leader	Ben Lynch benlynch@priorshallalc.com
Deputy Designated Safeguarding Leaders	Charlotte Brazier (EYFS and KS1 Leader) charlottebrazier@priorshallalc.com Justin Pye (KS2 Leader) justinpye@priorshallalc.com Jacqueline White (Inclusion Leader) jacquelinewhite@priorshallalc.com Alex Crawford (Nursery Lead Teacher) alexcrawford@priorshallalc.com Jenna Smith jennasmith@priorshallalc.com
Safeguarding Governor (including Online Safety)	Sue Gardner sgardner@iftl.co.uk
School Phone Number	01536 216090
Northamptonshire Multi-Agency Safeguarding Hub	0300 126 7000

1. Online safety and internet usage

1.1 Introduction

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and staff about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Priors Hall's Online Safety Policy operates in conjunction with other policies including those for Behaviour, Anti-Bullying and Child Protection.

1.2 Why is internet use important?

The purpose of internet use in school is to:

- raise educational standards
- to promote pupil achievement
- to support the professional work of staff
- to enhance the school's management information and administration systems

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Priors Hall has a duty to provide pupils with high quality internet access.

Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

1.3 How does internet use benefit education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums, libraries and art galleries to enhance the school's curriculum offer
- rapid and cost effective worldwide communication
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of
- networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority
- access to learning wherever and whenever convenient, especially during partial school closures (Remote Learning)
- greatly increased skills in literacy

1.4 How Can Internet Use Enhance Learning?

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils (3 to 11 years old)
- Children will be taught what internet use is acceptable and what is not, through computing and PSHE lessons
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

1.5 Good habits

Online safety depends on effective practice at a number of levels:

- Responsible computer and internet use by all staff and pupils, encouraged by education and made explicit through published policies
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the provider including the effective management of content filtering
- National Education Network standards and specifications

1.6 Dangers to consider

As outlined in Keeping Children Safe in Education 2021, the 4 Cs must be carefully considered:

- Content: engaging with or exposure to potentially harmfully content online
- Contact: experiences and/or targeted by potentially harmful contact online
- Conduct: witnesses, participates in and/or is a victim of potentially harmful conduct
- Contract: party to and/or exploited by a potentially harmful contract.

Some of the dangers children may face could include (but are not restricted to):

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through a robust educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with

these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. This Online Safety Policy outlines how we intend to do this.

2. Online Safety Audit

This quick self-audit will help the SLT, computing subject leader and DSL assess whether the Online safety basics are in place.

Has the school an Online Safety Policy that complies with CYPD guidance?	Yes
Date of latest update:	July 2021
The Policy was agreed by governors on:	1st September 2021
The policy is available for staff at:	Document available from the school office, on the school website and via the staff drive. Re-shared with all staff member annually (September)
And for parents at:	School website or paper copy from school office
Designated Safeguarding Leader (including Online Safety) is	Ben Lynch
Safeguarding Governor (including Online Safety) is	Sue Gardner
Has online safety training been provided for both pupils and staff?	Included into the computing curriculum and regularly reviewed in assemblies. Staff are trained in online safety in accordance with KCSIE 2021
Do all staff sign a computing and internet usage Code of Conduct on appointment?	Yes including governors
Do children sign an agreement about responsible IT use? Are parents sent a copy of that?	This is included in school planners for parents to read and sign alongside their child.
Have school Online safety rules been set for pupils?	Yes, these are called the SMART rules see Appendix E.
Are these rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access	Yes
Has the school filtering policy been approved by the SLT?	Yes – included in this policy (see section 3.5)
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?	Yes

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Broadband monitoring logs of internet activity (including sites visited) are provided through automatic notifications sent to the headteacher and Designated Safeguarding Leader when inappropriate content has been accessed
- Internal monitoring data for network activity
- Online safety co-ordinator in school and the online safety governor will meet regularly to review monitoring

3. Specific Safeguarding Considerations

Please see above key contacts when considering safeguarding concerns.

3.1 Internet Access and Responsibility

- All staff must read and sign the Staff Acceptable Computing and Online Use Agreement (Appendix A) before using any school computing resources, including laptops, IPads or school mobile phones
- Parents are informed that pupils will be provided with supervised internet access
- Parents will be sent a copy of the Pupil Acceptable Computing and Online Use Agreement which their children will have read with their teachers and signed in class (Appendix B)
- This agreement also applies to before and after school provisions in which children and adults may use computing equipment
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the Online Safety Co-ordinator and network manager (Aaron Wheeler at IFTL) who will investigate and take appropriate action, liaising with broadband provider if necessary
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

3.2 Email & Online Collaboration

- Pupils may only use approved email accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive messages
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Pupils may must not access others pupils' accounts or files
- Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use in person and virtually
- Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved.
- They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses
- Pupils must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use.
- Access in school to external personal email accounts may be blocked
- The forwarding of chain emails is not permitted

3.3 Social Networking

- At Priors Hall, we block/filter access to social networking sites and newsgroups unless a specific use is approved

- Pupils are advised never to give out personal details of any kind which may identify them or their location so that they safeguard themselves from exploitation or abuse
- Pupils are advised not to place personal photos on any social network space
- Pupils are advised on security and encouraged to set passwords on personal devices, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age. The following list is an indicator (but not exhaustive) of age limits:

  13+ age limit: Facebook, Instagram, TikTok, YouNow, House Party, Snapchat, Twitter, Kik.

  16+ age limit: WhatsApp

3.4 Cyberbullying

Definition: *"the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature".*

At Priors Hall, the same expectations of behaviour extend to interactions between staff, parents and children online. No form of discrimination, intimidation, prejudice or bullying will be tolerated. Staff, Senior Leaders, the Governing Body and children all have an awareness of what cyberbullying is and how they should deal with incidents. All incidents must be recorded on CPOMS so that they can be followed up by a member of the Safeguarding team, including incidents occurring outside of school.

Throughout the computing and PSHE curriculum, children are given the opportunity to understand how to interact positively with others and how to keep themselves safe online. This is reinforced through assemblies and anti-bullying awareness campaigns which enhance the curriculum offer.

Further resources to support the prevention of cyberbullying can be found at:

- www.internetmatters.org
- www.bullying.co.uk
- www.connectsafely.org
- www.safekids.com
- www.nspcc.org.uk

3.5 Filtering

The school will work in partnership with Internet Service Provider to ensure filtering systems are as effective as possible. Filtering systems are in place to ensure that inappropriate, abusive or extreme content is not accessible via the school system; however this is not 100% effective and all users should be aware of the potential harmful content online.

Web Filter reports are sent to the Headteacher and Designated Safeguarding Leader to address any potential abuse of internet usage. These reports are sent via email and stored in paper versions with safeguarding records and documentation.

Aaron Wheeler (IFTL) is the nominee responsible for updating and maintaining the filtering system. Aaron reports back any updates to the Headteacher and Designated Safeguarding Leader where appropriate.

3.6 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and their risks assessed
- Mobile phones will not be used for personal use during lessons or formal school time on the school site. See our Mobile Phone policy
- The sending of abusive or inappropriate text messages or photos (sexting) is forbidden
- Pictures should only be taken by staff on school owned devices such as IPads or work mobile phones.

3.7 Published Content & The School Website

- The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- Permission will be obtained from parents and carers, and kept on the school system, outlining which children are allowed to appear on the school's website

3.8 Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our technical support team and broadband provider if necessary
- Aaron Wheeler is the nominated member of staff responsible for information system security.

3.9 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. For further information, please see the IFTL GDPR and Data Protection Policy.

3.10 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit computing and online use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate

3.11 Handling online safety complaints

- Complaints of internet misuse will be dealt with by a member of the safeguarding team
- Any complaint about staff misuse must be referred to the headteacher as outlined by the Staff Code of Conduct and the Whistleblowing Policy
- These will be logged and dealt with as deemed appropriate by the head teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures
- Pupils and parents will be informed of the complaints procedure

3.12 Communication with All Stakeholders

Pupils

- Pupils will sign an Acceptable Use Agreement
- Rules for internet access will be posted in all classrooms
- Pupils will be informed that internet use will be monitored
- Pupils will be reminded of SMART Online Safety Rules regularly – especially when using the internet

Staff

- All staff will be given the Online safety Policy and its importance explained alongside annual updates
- Staff will sign an Acceptable Use Agreement
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the Online Safety Policy in newsletters, communication home and the school website
- Parents will receive a copy of their child's Acceptable Use Agreement

Priors Hall's Safeguarding Statement

Safeguarding is everybody's business. Priors Hall – a Learning Community has an unwavering commitment to safeguarding to ensure that: all our children and young people are safe and feel safe; that children, parents/carers and staff are able to talk about any safeguarding concerns and feel assured that they will be listened to; and that all staff and volunteers are aware of and implement safeguarding procedures and guidance, including what to do if they suspect a child or young person may be experiencing, or be at risk of harm. In essence, we instil a culture of vigilance.

All concerns should be given to our school Designated Safeguarding Leads: **Ben Lynch (DSL), Tess McQuade (Headteacher and DDSL), Justin Pye (KS2 Lead and DDSL), Charlotte Brazier (EY/KS1 Lead and DDSL), Jacqueline White (Inclusion Lead and DDSL), Alex Crawford (Nursery Lead Teacher and DDSL) and Jenna Smith (DDSL).**

- In any case where an adult is concerned that a child is, or may be, at risk of significant harm they must report this immediately to the DSL or to a member of the Safeguarding Team who will make a referral directly to Northamptonshire Multi-Agency Safeguarding Hub (MASH) on **0300 126 7000**.
- If a child or other person is at immediate risk of harm, the first response should always be to call the police on **999.** This policy applies to all adults, including volunteers, working in or on behalf of Priors Hall – a Learning Community.
- If a concern is in relation to a member of staff at Priors Hall (who is not the Headteacher), please contact Tess McQuade on **01536 216090** ext **303** to report this concern. If a concern is in relation to the Headteacher, please contact the Chair of Governor (Sue Gardner) via email on sgardner@iftl.co.uk or IFTL Safeguarding Lead (Kim Kemp) via email on kimkemp@iftl.co.uk.

Appendices

Appendix A

Staff and Governor Acceptable Use Agreement

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.

1. Aims & Background

This online and computer user agreement covers the use of all digital technologies supplied by and used while in school: email accounts, internet usage, intranet access, network resources, learning platforms, software usage, communication tools, social networking, school website, apps and other relevant digital systems.

This user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school, such as VPN or webmail, or other systems providers when accessed from outside school.

Any posts made on a non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute is also included in this agreement.

The school regularly reviews and updates all policies to ensure they are consistent with current legislation and guidance.

2. User Requirements

School employees, governors, and third-party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures.

Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

By signing this agreement, you agree to:

1) Only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body in the line of my employment.
2) Set strong passwords, following advice provided by the school which are regularly changed and not shared with anyone else.
3) Not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system which is accessible as a member of staff at Priors Hall.
4) Ensure all documents and data are handled in accordance with IFTL's GDPR policy.
5) Not engage in any online activity that may compromise my professional responsibilities.
6) Only use the schools approved email system(s) for any school business.
7) Only use the approved method/s of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.
8) Not support or promote extremist organisations, messages or individuals and will not give a voice or opportunity to extremist visitors with extremist views, either in person or virtually.

9) Not browse, download or send material that is considered offensive or of an extremist nature by the school.

10) Report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher or Designated Safeguarding Leader.

11) Not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

12) Check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

13) Not connect any device (including USB flash drive) to the network that does not have up-to date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended antivirus and other malware systems.

14) Not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

15) Follow the school's policy on use of mobile phones/devices at school.

16) Only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure photographs and videos of children and staff are saved on the staff-only drive within school.

17) Only take or publish images of staff and students with their permission and in accordance the school's consent guidelines. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

18) Use Teams or Zoom as the school's Remote Learning Platform in accordance with the instructions provided by Senior Leaders.

19) Ensure that any private social networking sites, blogs, etc. created or actively contribute to are not confused with my professional role, and will create a distinction between the two. Measures will be taken to protect personal social media accounts (privacy settings) to protect the professionalism of Priors Hall and individuals.

20) Agree and accept that any device loaned to me by the school is provided solely to support my professional responsibilities.

21) Only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.

22) 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.

23) Understand that data protection policy requires that any information seen by me with regard to staff or pupil 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 (e.g. safeguarding concerns).

24) Be aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

25) Understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way to the Headteacher following the Whistleblowing Policy.

26) Understand that all internet and network traffic / usage can be logged and this information can be made available to the Headteacher or Designated Safeguarding Lead on their request.

27) Understand that internet encrypted content (via the https protocol) may be scanned for security and/or safeguarding purposes.

28) Understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

29) Embed the whole school approach to online safety throughout teaching practice.

3. Links with Other Policies

I understand that this user agreement is linked to the schools:

- GDPR and Data Protection Policy (IFTL)
- Child Protection Policy (Priors Hall)
- Whistleblowing Policy (IFTL)

4. Agreement Form

I agree to abide by all the points above. I understand that I have a responsibility for my own and others' online safety and I undertake to be a 'safe and responsible online and computer user'. 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 and Child Protection Policy. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature _____ Date _____

Full Name _____ (printed)

Job title / Role _____

Appendix B

Child Acceptable Use Agreement

Acceptable Use Agreement for EYFS and KS1

- I will only use the internet or computer when a teacher or adult is with me
- I will only use my own login and password and I will not tell anyone else what it is
- I will not look at or delete other people's files
- I will not bring in memory sticks from home without permission
- If I see anything that upsets me, I will tell an adult
- I will not give out any details about me, like my name or address
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers at Priors Hall

Acceptable Use Agreement for KS2

- I will use the school computers and technology sensibly and safely
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages to others
- I will not give out my personal information, speak with people I do not know or arrange to meet anyone online
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers.

Appendix C

Letter sent home to parents (KS2 example)

Dear Parents

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At Priors Hall, we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. Social networks have no place in our school and so school staff should not be approached by pupils or parents online or invited to join.

Your child has read the following **Acceptable Use Agreement** in class with their teacher. Once they have fully understood them all, your child has signed their name to agree to stick by them. Please read them again at home with your child to show your support of the school in this important aspect of our work. Thank you.

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

Appendix D

Use of technology in school

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones				*				*
Use of school hand held devices eg iPads	*						*	
Use of personal email addresses in school, or on school network	*							*
Use of chat rooms/facilities				*		*		
Use of instant messaging				*		*		
Use of social networking sites				*				*
Use of blogs				*		*		
Use of secure learning platforms to collaborate	*				*			

When using email the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report, to the nominated person (Aaron Wheeler) the receipt of any email or electronic message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and parents must be professional in tone and content. This should happen only via email or ClassDojo.

- Children should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix E

SMART Online Safety Rules