Hayes School Online safety Policy

Owner (job role):	Chief Operating Officer (COO)
Approval Body:	Resource and Finance Committee
Approval Date:	11 March 2025
Implementation Date:	12 March 2025
Date of last review:	N/A (new Trust Policy)
Date of next review:	March 2027

Version	Approval date	Summary of changes
1.0		New version of policy

Inspire, Respect, Flourish.

1 Contents

2 Our Vision and Values

Together, we enable everyone to thrive.

- Ambition – we have high aspirations for our children and strive to do our very best.
- Inclusion – we care about the whole child and everyone will feel that our Trust is a place where they are valued, respected, safe and happy.
- Collaboration – we are stronger together and collaborate generously to ensure the long-term success of our children, our staff, our schools and the communities we serve.
- Trust – we build trust by acting with integrity and kindness and by putting children first.

3 Important Contacts

ROLE/ORGANISATION	NAME	CONTACT DETAILS
Trust-level		
Chair of trustees	John Phillipson	c/o Leona Eley leley@imat.uk
Link Trustee for safeguarding	Kieran Osborne	c/o Leona Eley leley@imat.uk
Chief Executive Officer	Sarah Lewis	info@imat.uk
Local / National Support		
Bromley Local Authority Designated Officer (LADO)	Gemma Taylor	0208 461 7775 or 0208 313 4325 lado@bromley.gov.uk
Bromley Local Authority Safeguarding Officer	Libby Kember	0208 313 4665 Mobile 07974 870 800 Libby.kember@bromley.gov.uk
Urgent safeguarding referrals should be made to: Bromley Children and Families Hub	N/A	020 8461 7373 / 7379 / 7026 access the portal to make a referral Bromley Children's Portal Out of Hours (emergencies only): 5.00pm – 8:30am and weekends: 0300 303 8671
Extremism in Schools Helpline for Teachers	N/A	0207 340 7264 Counter.extremism@education.gov.uk
School Name Here		
Designated Safeguarding Lead (DSL)		
Deputy Safeguarding Lead (DDSL)		
Online Safety Lead		
Chair of Local Governing Body		
Local Governing Body for Safeguarding		

4 Introduction

The trustees and governors of Impact Multi Academy Trust are committed to safeguarding and promoting the welfare of children and young people and require all staff and volunteers to share this commitment to a whole-school and whole-Trust approach to safeguarding.

This policy complies with our funding arrangement and articles of association and will be reviewed and updated annually.

5 Aims

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

6 Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

7 Roles and Responsibilities (R&Rs)

7.1 The Board of Trustees

The Trust board will facilitate a trust-wide approach to safeguarding, ensuring that safeguarding and child protection are at the forefront and underpin all relevant aspects of process and policy development.

The Trust board will:

- Evaluate and approve the policy at each review
- Appoint a link Trustee for safeguarding to monitor the effectiveness of this policy in conjunction with the full Trust board and to work with safeguarding link governors to support effective practice across the Trust
- Ensure all Trustees and local governors read Keeping Children Safe in Education and complete training on induction and at regular intervals

7.2 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The LGB will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LGB will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The LGB should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The LGB in collaboration with the Trust Central Team (COO & Trust Technology Officer) and Headteacher, must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with the COO and TTO (who are responsible for decision making and implementation) what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

7.3 The Chief Executive Officer

The CEO will:

- Ensure an annual safeguarding audit (which includes online safety) is carried out in each of the trust schools
- Support the COO, Director of Education and Headteachers in ensuring remedy of deficiencies in the school's and trust's safeguarding systems without delay, where necessary.

7.4 The Chief Operating Officer & Trust Technology Officer

The COO, supported by the TTO will:

- Ensure that this policy is reviewed at least annually (and in response to any changes in guidance or lessons learned).
- Remedy deficiencies in the trust's IT systems responsible for filtering and monitoring without delay
- In collaboration with the LGB and Headteacher, ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The COO & TTO will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

7.5 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Headteacher will:

- Ensure staff are trained on their expectations, roles and responsibilities around filtering and monitoring systems
- Work with ICT Managers, COO and Trust Technology Officer to make sure the appropriate systems and processes are in place for filtering and monitoring

- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation

7.6 The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the LGB to ensure the procedures and implementation are updated and reviewed regularly
- Understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with ICT Managers, the COO and Trust Technology Officer to make sure the appropriate systems and processes are in place
- Working with ICT Managers and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged using CPOMS/MyConcern as appropriate
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or LGB and/or COO
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

7.7 ICT Managers

ICT Managers are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

7.8 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Understanding the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures by informing the DSL if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the DSL to ensure that any online safety incidents are logged using CPOMS/MyConcern and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Trust behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

All staff can bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present.

This list is not intended to be exhaustive.

7.9 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet
- The wellbeing hub login

7.10 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it.

8 Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

9 Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via the school website and other forms digital communication tools or platforms (Bromcom/VLEs). This policy will also be shared with parents/carers.

Elements of Online safety may also be covered during parent/carer events.

The school will let parents/carers know how online safety is covered in the curriculum

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Class teacher DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

10 Cyber-Bullying

10.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the trust behaviour policy.)

10.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers receive safeguarding training which includes addressing bullying.

The school may also send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the trust behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

10.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Our trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully pupils very seriously, in line with our trust behaviour policy.

11 Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. The trust maintains a Bring Your Own Device Policy (BYOD), the terms of which also apply.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

12 Pupils using Mobile Devices in School

12.1 Mobile devices in Impact Trust Secondary schools

Students are allowed to bring mobile phones to and from school. Mobile telephones are banned during the academic day, Appendix B of the Trust behaviour policy details the arrangements for mobile telephones in each individual secondary school.

12.2 Mobile devices in Impact Trust Primary schools

Only pupils in Year 6 are allowed to bring mobile telephones to and from school. Pupils in Years 5 and below are not allowed to bring mobile telephones on site. Mobile telephones are banned during the academic day and are collected at the start of the school day and secured safely in the school office until the end of the school day. Children are expected to turn their phone off on arrival to school and are not to use their phone to contact parents/carers directly whilst on the school site. Owning a mobile phone is not a requirement for a child to be allowed to walk home by themselves.

13 Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the Staff AUP and BYOD policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from their line manager.

14 How the School/Trust will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow our trust behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary policy and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

15 Training

15.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

16 Monitoring Arrangements

Staff log behaviour and safeguarding issues related to online safety using CPOMS/MyConcern

This policy will be reviewed every year by the Chief Operating Officer (COO) and Director of Education (DoE). At every review, the policy will be shared with the trust board. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

17 Links with Other Policies

This online safety policy is linked to our:

- Trust Safeguarding policy
- Trust Behaviour policy
- Staff Disciplinary policy
- Staff Code of Conduct
- Data Protection policy and Privacy Notices
- Complaints Procedure

18 Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

19 Appendix 2: KS2, KS3, KS4 and KS5 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

20 Appendix 3: acceptable use agreement (Staff, Governors, Volunteers and Visitors)

Please see the separate **Technology (IT) Acceptable Use Agreement – Staff** policy.