ONLINE SAFETY POLICY

Version	4.0
Approved By	Trust Board
Issue Date	20 September 2023
Review Date	October 2024

REVIEW HISTORY

VERSION NO.	DATE OF CHANGE	CHANGE SUMMARY	REF.
2.0	29.3.21	Branding	
3.0	26.4.22	Added Bring Your Own Device section	
3.0	26.4.22	Comments from DPO	p.14
4.0	13.02.23	Rebranding	
5.0	17.04.23	Retitled Online Safety Policy – to include device loan agreements in appendices	

Table of Contents

Purpose 4
Legislation and guidance 4
Roles and responsibilities 5
Educating pupils about online safety 7
5. Educating parents about online safety 9
6. Cyber-bullying 9
7. Acceptable use of the internet in school 12
8. Pupils using mobile devices in school 12
9. Staff using work devices outside school 13
10. Bring Your Own Device Considerations – Staff 13
11. How the trust will respond to issues of misuse 14
12. Training 14
13. Monitoring arrangements 15
14. Links with other policies 16
Appendix 1: EYFS and KS1 acceptable use and loan agreement (pupils and parents/carers) 17
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) 18
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 20
Appendix 4: Device Loan Agreement (Pupils) 21
Appendix 5: Device loan agreement for staff 23
Appendix 6: online safety training needs – self-audit for staff 25
Appendix 7: online safety incident report log 26

Purpose

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- 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

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 schools
- 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.

This policy complies with our funding agreement and articles of association.

Data will be processed to be in line with the requirements and protections set out in the UK General Data Protection Regulation 2018.

Roles and responsibilities

1.1 The Board of Trustees and Local Governing Bodies

The Board of Trustees has overall responsibility for monitoring this policy and holding the Executive Team to account for its implementation.

The Director of School and People Development will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

Local Governing Bodies

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the trust'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 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;

1.2 The Headteacher

The headteacher of each school is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

1.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in each individual school's child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;

- Working with the headteacher, ICT manager 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 child protection policy;
- Ensuring that any online safety incidents are logged (see appendix 7) and dealt with appropriately in line with this policy;
- 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 (appendix 4 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the headteacher and/or governing board;

This list is not intended to be exhaustive.

1.4 The Managed Service Provider (MSP)

The MSP is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting full security checks and monitoring the trust's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see appendix 7) and dealt with appropriately in line with this policy;

This list is not intended to be exhaustive.

1.5 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 trust's ICT systems and the internet (appendix 3), and ensuring that pupils follow the trust's terms on acceptable use (appendices 1 and 2);
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 7) and dealt with appropriately in line with this policy;

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and the trust anti-bullying 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';

This list is not intended to be exhaustive.

1.6 Parents

Parents 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 trust's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

1.7 Visitors and members of the community

Visitors and members of the community who use the trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study. Academies that don't follow the National Curriculum should adapt this section to include details of how online safety forms part of their own curriculum.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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 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 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;

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;

In **Key Stage 3**, 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 **Key Stage 4** 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 which 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 which 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);

All schools

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.

5. Educating parents about online safety

Each school will raise parents' awareness of internet safety in letters or other communications home, and in information via their website and social media. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use;
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online;

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

Concerns or queries about this policy can be raised with any member of staff, the headteacher or the trust Director of School and People Development.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the anti-bullying policy.)

6.2 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 schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their students.

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 (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that 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 school 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or;

- Is identified in the school rules as a banned item for which a search can be carried out, and/or;
- Is evidence in relation to an offence;

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL;
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- Seek the pupil's cooperation;

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or;
- Undermine the safe environment of the school or disrupt teaching, and/or;
- Commit an offence;

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or;
- The pupil and/or the parent refuses to delete the material themselves;

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image;

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Our trust anti-bullying policy and the school's behaviour policy;

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, trustees and governors are expected to sign an agreement regarding the acceptable use of the trust's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the trust's terms on acceptable use if relevant.

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.

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

8. Pupils using mobile devices in school

In the interests of safety during the journey to school, pupils may bring mobile devices onto site, but are not permitted to use them during the school day without express permission.

This also extends to clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Keeping operating systems up to date by always installing the latest updates;

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 the MSP.

10. Bring Your Own Device Considerations – Staff

The Trust recognises that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Where appropriate, 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;
- Where necessary, installing anti-virus and anti-spyware software;
- Keeping operating systems up to date by always installing the latest updates

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

11. How the trust will respond to issues of misuse

Where a pupil misuses the trust's ICT systems or internet, 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 trust'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 procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

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.

To ensure that the Trust complies with RPA insurance requirements, all employees or governors will undertake NCSC Cyber Security Training and share their completion certificate with the school. The Trust notes that this completion evidence will be required in the event of any claim relating to cyber security.

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, 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 in each school 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 and trustees 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 the school child protection and safeguarding policies.

13. Monitoring arrangements

Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

The Trust will utilise a 3rd party support service (such as Smoothwall monitor) to enhance its monitoring provision for all Trust supplied devices. This service will provide real-time monitoring for schools in addition to the filtering support from the MSP. Headteachers will receive regular updates on filtering within their school as well as direct contact from the 3rd party where an immediate risk is identified.

With regard to monitoring trends, within the Trust and individual use by staff and pupils, the Trust will audit the use of the Internet and electronic mail to ensure compliance with this policy. The monitoring practices of the Trust are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g., bullying (see anti-bullying policy for further information). We will also ensure that staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently subjected to harm.

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 7.

The DSL will meet at least annually with the Governor responsible for safeguarding, the lead for cyber security in school and a member of the MSP support team to check the

monitoring provision and procedures are working as expected. They will also record decisions regarding any black or whitelisted websites or applications.

The Trust has registered with Police Cyber Alarm. This connects Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data.

This policy will be reviewed every year by the Board of Trustees. The review will be supported by a regular risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to trust/school:

- Child protection and safeguarding policy (individual schools)
- Behaviour policy (individual schools)
- Disciplinary policy
- Data protection policy and privacy notices
- Anti-bullying policy

Appendix 1: EYFS and KS1 acceptable use and loan 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: o I click on a website by mistake o I receive messages from people I don't know o 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:**

Appendix 2: KS2, KS3 and KS4 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 which 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 in school time, at 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.	

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way which could harm the school's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Share my password with others or log in to the school's network using someone else's details Take photographs of pupils without checking with teachers first Share confidential information about the school, its pupils or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Device Loan Agreement (Pupils)

We are loaning you this device ("the equipment") for the benefit of your child in supporting and developing their education. This agreement sets the conditions for taking the equipment.

1. The loan agreement exists between the school and the Named Person who has signed this loan agreement.

Pupil Name:

Parent/Carer's Name & Address:

Device name or number:

The agreement governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school. All issued equipment shall remain the sole property of the school.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement. I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the Managed Service Provider via the school, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy if the pupil engages in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact the managed service provider on the email helpdesk@aitn.co.uk

6. Return date

I will return the device in its original condition to the school office within ten days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

Appendix 5: Device loan agreement for staff

1. The loan agreement exists between the school and the Named Person who has signed this loan agreement.

Name:

Address:

Device name or number:

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the employee a device ("the equipment") for the purpose of working from home.

2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is [damaged, lost or stolen], I will immediately inform the Managed Service Provider (AIT), and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community

- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the trust's policies on staff discipline.

4. Personal use

I will not use this devise for any personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected:

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Make sure the equipment locks if left inactive for a period of time;
- Do not share the equipment among family or friends;
- Update antivirus and anti-spyware software as required;
- Install the latest updates to operating systems, as prompted;

If I need help doing any of the above, I will contact AIT on helpdesk@aitn.co.uk.

6. Return date

I will return the device in its original condition to the school office within ten days of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

7. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME	
SIGNATURE	
DATE	

Appendix 6: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 7: online safety incident report log

online safety incident log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**