School Online Safety and Cyber Security Policy

Date First Published	September 2020
Version	2
Last Approved	September 2023
Review Date	September 2024

Contents

Changes to this edition 4
1. Purpose and Aims 5
2. Links to other documents 5
3. Roles and responsibilities 6
3.1 Trust Board 6
3.2 The Headteacher 6
3.3 The Designated Safeguarding Lead & Online Safety Lead 7
3.4 The Online Safety Lead 7
3.5 IT Support Services 8
3.6 All staff and volunteers 8
3.7 Parents 9
3.8 Students 9
4. Educating students about online safety 10
5. Educating parents about online safety 11
6. How the school will respond to issues of misuse and online safety incidents 11
7. Child-on-child sexual abuse and harassment 12
8. Cyber-bullying 12
8.1 Definition 12
8.2 Preventing and addressing cyber-bullying 13
8.3 Examining electronic devices 14
9. Cyber-crime 14
10. Acceptable use of the internet in school 15
11. Passwords 15
12. Filtering internet access 16
13. Managing IT systems and access 16
14. Learning technologies in school 16
15. Staff using work devices outside school 18
16. Student Remote Learning 18
17. Training 19
18. Recording and reporting 19
19. Monitoring and evaluation 19

20. Equality Impact Assessment 19
Appendix 1: Acceptable Use Agreement (students and parents/carers) 21
Foundation/ KS1 Student Acceptable Use Policy Agreement ..... **Error! Bookmark not defined.**
KS2/3/4/5 Student Acceptable Use Policy Agreement 22
Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors) 23
Appendix 3: Online Safety Training Needs – Self-audit for staff 25
Appendix 4: Online Safety Curriculum Overview 26

Changes to this edition

This policy has been updated in September 2023. It represents a significant re-write to previous versions and consolidates the previous policy.

1. Purpose and Aims

The school recognises the immense benefits that IT, the internet and a wide range of electronic communication devices and social media platforms that provide for the development of high-quality learning experiences across our school community.

We wish to actively promote engagement in the range of technologies available throughout our whole school community. With the advent of student and parental engagement through Parent Portal, a whole new level of communication and active engagement is available to us which enables us to operate within a wholly transparent and cohesive learning environment.

The school also recognises the need to balance the benefits of these technologies bring to the personal, social and health education of our students with a thorough awareness of the potential risks. It is vital that our whole school community understands and adheres to the online safety policy that ensures safe, appropriate and responsible use of such technologies and reduces the risk of exposure to adverse media and the potential impact on the mental health and wellbeing. This policy is designed to reflect our commitment to the safeguarding and wellbeing of our students.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Links to other documents

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2023'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Low-level Safeguarding Concerns Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy (if applicable)
- RSE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Staff Code of Conduct
- Behaviour and Exclusions Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Student Remote Learning Policy

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

3. Roles and responsibilities

3.1 Trust Board

The Trust Board has overall responsibility for monitoring this policy and ensuring it complies with relevant laws and statutory guidance, holding the Executive Team and headteacher to account for its implementation and ensuring all staff undergo relevant training to support its implementation.

3.2 Executive Team

The Executive Team have overall responsibility for developing this policy and ensuring its implementation in all schools and areas of the Trust; ensuring appropriate training and support is provided on an annual basis for all staff, students, parents/carers and Local Governors.

3.2 The Headteacher

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL, deputy DSL and Online Safety Lead by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated and that the policy is being implemented consistently across the school.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Ensuring the Safeguarding Lead Governors are engaged is involved in the monitoring and impact of this policy.

3.3 The Designated Safeguarding Lead

- The designated safeguarding lead has responsibility for safeguarding and child protection which includes online safety and understanding the filtering and monitoring systems and processes in place
- Working closely with the Online Safety Lead to implement this policy.
- Keeping up-to-date with current research, legislation and online trends.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Working with the Online Safety Lead to establish a procedure for reporting, recording and dealing with online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing body about online safety on a termly basis.
-

3.4 The Online Safety Lead

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the DSL to establish a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff
- Ensuring all members of the school community understand the reporting procedure
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Updating (on a regular basis) and delivering staff training on online safety which includes an understanding of the expectations, applicable

roles and responsibilities in relation to filtering and monitoring. (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring a robust and high quality Online Safety curriculum is planned and delivered as set out in Appendix 5
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- 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.

3.5 IT Support Services

Those with responsibility for managing the school network are responsible for:

- Responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard all systems,
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 weekly basis
- 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 4) 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

This list is not intended to be exhaustive.

3.6 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 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS as per safeguarding procedures 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

This list is not intended to be exhaustive. Please note that any visitors to school who may be shadowing or supporting a department must only access the school network under supervision of a member of staff. Supply staff and volunteers who work in school regularly will receive briefing on online safety prior to being issued with logins and passwords to enable them to access the system independently. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

3.7 Parents

Parents are expected to:

- Help and support your school in promoting online safety
- Read, understand and promote the school student Acceptable Use Policy with your children
- Take responsibility for learning about the benefits and risks of using the Internet and other social media platforms and technologies that your children use in school and at home
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss online safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology and online platforms
- Model safe and responsible behaviours in your own use of technology
- Consult with the school if you have any concerns about your children's use of technology
- 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 (appendix 1).

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

- What are the issues?, UK Safer Internet Centre: Link
- Hot topics, Childnet International: Link
- Parent factsheet, Childnet International: Link

3.8 Students

All students are expected to:

- Abide by the school's acceptable use policy
- Ensure they use technology in a safe and responsible manner
- Protect their own passwords and personal information

- Notify a member of staff if they have concerns about themselves or other students
- Report any incidents and concerns in line with this policy.

4. Educating students about online safety

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings. We will provide a series of specific online safety related lessons in every year group as part of the curriculum. We will celebrate and promote online safety through planned assemblies.

We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

We will ensure that all students are made aware of where to seek help or advice or make a report if they experience problems when using the internet and related technologies including social media.

We will remind students about their responsibilities through an end-user Acceptable Use Policy which every student must agree to, to allow them to use a device on first log on. The student Acceptable Use Policy will be displayed in each IT suite and displayed when students log on.

Staff will model safe and responsible behaviour in their own use of technology during lessons.

Students across all key stages will be taught using a spiralised curriculum which grows in depth and age-appropriate content. An overview of this can be found in the Appendix 5. This will be quality assured in line with the school's quality assurance procedures.

Online Safety is taught through a combination of discrete lessons and when appropriate throughout the curriculum; including Tutor Time and Assemblies. Discrete online safety lessons are identified within our Computing, RSHE or PD lessons. Appropriate resources are available through our National Online Safety membership.

The school will report any potential risks and will ensure that online safety is considered consistently through planning the curriculum, staff training, the work of the designated safeguarding lead and parental engagement. The school has a specific policy for remote learning provision.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety awareness for parents will also be supported through use of the National Online Safety programmes and associated resources.

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.

6. How the school will respond to issues of misuse and online safety incidents

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the 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 procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour should be reported in line with the procedure set out in the school's Child Protection and Safeguarding Policy.

Concerns regarding a student's online behaviour should be reported to the DSL, who should investigate and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

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

The school avoids unnecessarily criminalising students, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal

developmental curiosity, e.g. a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response should be recorded by the DSL on CPOMS.

7. Child-on-child sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. This access means some children, whilst at school, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. As a school we carefully consider how this is managed on our premises and as such this is reflected in both our mobile and smart technology policy and our child protection and safeguarding policy.

Staff understand that this abuse can occur both in and outside of school, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

8. Cyber-bullying

8.1 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.

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages

- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain students can be more at risk of abuse and/or bullying online, such as LGBTQ+ students and students with SEND.

Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the school's Behaviour & Exclusions Policy and Anti-bullying Policy.

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, 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 groups, and the issue will be addressed in assemblies.

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 students, as part of safeguarding training (see section 14 for more detail).

The school may also send 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 or may utilise the resources available through the National Online Safety programme.

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 students, the school will use all reasonable endeavours to ensure the incident is contained and reported to the necessary authorities.

The DSL and Online Safety Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on https://www.gov.uk/government/publications/searching-screening-and-confiscation and the school's policy on Screening, Searching and Confiscation.

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

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or

inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Acceptable use of the internet in school

All students, parents, 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 and 2). Visitors will be expected to read and agree to the school'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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the Acceptable Use Agreement in Appendices 1 and 2.

11. Passwords

A secure and robust username and password protocol exists for all system access. Staff and students will have a unique individually named user account and password for access to IT available within the school and via remote access. All staff and students have a responsibility for the security of their username and password.

In line with current password guidance from the National Cyber Security Centre, the password policy for staff, visitors, governors and students is as follows:

- Passwords with have a minimum of 12 characters.
- There is no requirement to use specific characters or to change the password at certain intervals.
- Passwords to school computers and Microsoft or Google services must be unique and not used for other systems.
- Best practice is to use passwords with three random words.

In line with staff and student Acceptable Use Policies users must not allow other users to access systems using their log on details and must report any suspicion or evidence of any breach of security. Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow students to access the Internet through their log-on. They will abide by the school Acceptable Use Policy at all times.

12. Filtering internet access

The school uses an Internet service provided by the LA. The filtering is delivered using a Smoothwall web filter device. If users discover a website with inappropriate or potentially illegal content, this should be reported to a member of staff who will inform a member of IT Support Team.

The IT Support Team will report, record and adjust filtering as required. The school uses software to monitor all user's activity on the school's workstations. The IT Support Team have access to AB Tutor to review and investigate any issues. If required, reports will be made to the Safeguarding Team and, to appropriate agencies. The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

13. Managing IT systems and access

The school will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible. The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date. The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

By using any school device or device in school, all users agree an end-user Acceptable Use Policy provided by the Trust (see Appendix 1 and 2). Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school IT systems and, that such activity will be monitored and checked.

The school will audit IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate on an annual basis. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

Details of all IT equipment, including hardware and software will be recorded in a school inventory. All redundant IT equipment will be thoroughly checked to ensure all school related information including personal or school specific information has been thoroughly removed. All redundant IT equipment will be disposed of appropriately, including recycling with partner primaries where possible. All IT assets written off must be notified to central finance (finance@minervalearningtrust.co.uk) for noting on the asset register and reporting to Trust Board.

14. Learning technologies in school

The school has a clear policy on the use of mobile and smart technology, which also reflects the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). Any use of mobile devices and smart technology by students must be in line with the Acceptable Use Agreement (see Appendix 1). Any breach of the acceptable use agreement by a

student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Our policy on staff and student use of a range of learning technologies is summarised in the following table. Staff and students should also refer to the Acceptable Use Policy whenever engaging with such technologies.

	Students	**Staff**
Student/Staff Personal mobile phones brought into school outside	Students allowed for use outside of school site only	Staff allowed in appropriate places at appropriate times
Mobile phones used in lessons	Students not allowed	Staff not allowed unless with permission in exceptional circumstances for private calls.
Bring your own device (BYOD)	Is not permitted.	Is permitted in line with School policy and ensuring security of the network is maintained
Smart devices	Students not allowed unless for learning purposes	Staff allowed as part of learning activity or with permission in exceptional circumstances for private calls/use
Taking photographs or videos on personal equipment	Students not allowed	Staff not allowed
Taking photographs or videos on school devices	Students allowed with permission as part of a learning activity. There must be prior consent from the student under GDPR	Staff allowed as part of teaching activity. Staff Acceptable Use Policy must be followed. Prior consent by the student is required under GDPR.
Use of personal email addresses in school	Students not allowed. Students are provided with school email address that should be used for learning activities.	Staff allowed as long as the IT Acceptable Use Policy is followed

Use of school email address for personal correspondence	Students allowed as long as the IT Acceptable Use Policy is followed	Staff allowed as long as the IT Acceptable Use Policy is followed
Use of Social Media	Students not allowed	Staff not allowed unless it is related to school social media accounts.
Use of Web Services	Students allowed with permission as part of a learning activity as long as the IT Acceptable Use Policy is followed	Staff allowed as part of a school-based activity as long as the IT Acceptable Use Policy is followed

15. Staff using work devices outside school

Work devices must be used solely for work activities. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices or other portable media containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Online Safety Lead.

16. Student Remote Learning

All remote learning is delivered in line with the school's Remote Learning Policy. School devices may be loaned to students where appropriate. These devices currently have no internet filtering or monitoring when used offsite. Students are expected to use within the terms of the Acceptable Use Policy.

Where students are expected to use online resources from home, on school or personal devices, parents and carers should be made aware of what students are being asked, including online tasks and websites the students are being asked to use. Parents and carers should also be made aware of any school staff with whom students will be interacting online, and how they might be contacted.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.

- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

17. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, 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. This is done as part of our National Online Safety membership. Staff will also receive regular updates via the safeguarding newsletters, safeguarding briefings and e-bulletins to continue to provide them the the revenant skills and knowledge to safeguard students effectively.

The DSL and deputy 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. In line with the requirement of the Sheffield Children's Safeguarding Partnership, the online safety co-ordinator will be trained to the same level as the DSL.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. This will take place on an annual basis. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

18. Recording and reporting

The Online Safety Lead will log behaviour and safeguarding issues related to online safety via CPOMS which is a secure online safeguarding system.

The DSL will ensure that all relevant issues are logged on a child's CPOMS records and that any appropriate action to keep children safe in taken in line with Keeping Children Safe in Education (2023) and the school's Child Protection and Safeguarding Policy.

19. Monitoring and evaluation

This policy will be reviewed annually in line with any statutory changes and approved by the Trust Board.

20. Equality Impact Assessment

The Trust will carry out an Equality Impact Assessment in order to ensure that policies, procedures and practices cater for individuals who share protected characteristics in relation to the Equality Act 2010. The purpose of these assessments is to ensure that policies, procedures and practices within the organisation are fair to all. If unfairness is highlighted, the assessment will also seek to show how this can be changed and, where it can't be changed, how it can be improved.

The Trust will monitor the impact of the policy to assess whether there is evidence of a detrimental impact on anyone with a protected characteristic as a result of the application of this policy. The assessment will include consideration of adaptations or changes which can be made to address any issues identified.

Appendix 1: Acceptable Use Agreement (students and parents/carers)

Think before you click	
S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

KS2/3/4/5 Student Acceptable Use Policy Agreement

Acceptable use of the IT systems in school and internet, or school IT systems offsite: agreement for students and parents/carers.

This policy covers the use of all school-owned IT provision (e.g. computers, wifi networks, mobile devices) and use of personal technology on the school site. The use of school-owned IT provision is granted to students as a privilege and it is for educational use only. If students choose to use their own devices in school, they must follow the rules set out in this agreement, in the same way as if I was using school equipment. By using any IT system or device , students agree the following.

When using the school's ICT systems and accessing the internet in school:

- My behaviour online is always of a high standard.
- I only use IT systems for educational purposes.
- I use them with a teacher being present, or with a teacher's permission.
- I only access appropriate websites.
- I only access social networking sites when my teacher has expressly allowed this as part of a learning activity.
- I only open any attachments in emails, or follow any links in emails, after first checking with a teacher I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I always use appropriate language when communicating online, including in emails.
- I keep my password safe and secure and only log in to the school's network using my own credentials.
- I keep my personal information safe and secure (including my name, address or telephone number) only sharing such information with the permission of my teacher or parent/carer.
- I only arrange to meet anyone offline after first consulting my parent/carer, or with adult supervision.
- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I always check that any information I use online is reliable and accurate.
- I make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- My use of personal devices in school, including, but not exclusively, mobile phones and personal laptops, is within the specific school policy.
- I immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I know that if I break the rules I might not be allowed to use school systems.

I will always use the school's ICT systems and internet responsibly.

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Trust and School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, all staff, governors, volunteers and visitors are expected to have read the Acceptable Usage Policy (AUP) and by using any IT systems they are agreeing to abide by the policy.

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Minerva Learning Trust expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Minerva Learning Trust both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies**.**

I understand that the Acceptable Usage Policy (AUP) should be read and followed in line with the Trust staff code of conduct, and that by using any IT systems in school, I am agreeing to abide by this policy.

I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Trust ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Security and Practice

When using the trust's ICT systems, or my own devices with permission, and accessing the internet in school, or outside school on a work device:

I only use the trust'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, excluding but not limited to material of a violent, criminal or pornographic nature.

I only use IT systems in any way which could not harm the trust's or school's reputation. I do not access social networking sites or chat rooms, unless as an agreed part of my role. I always use appropriate language when communicating online, including in emails or other messaging services.

I agree that the trust will monitor my IT system use and the websites I visit.

I do not attempt to bypass any filtering and/or security systems put in place by the trust and I will report any filtering breaches to the Online Safety Lead and the designated safeguarding lead (DSL).

I keep all passwords safe and secure and only log in to each school's network using my own credentials. I lock my device when left unattended.

I 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 trust's data protection policy. All portable storage devices I use are encrypted and are used in accordance with school policies.

I will let the Online Safety Lead and the designated safeguarding lead (DSL) know if a student 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.

If I lose any trust or school related documents or files, I will report this to IT support and the school or trust Data Protection Officer as soon as possible.

I always use the trust's ICT systems and internet responsibly and ensure that students in my care do so too.

I only install authorised software, including browser toolbars and add-ons.

I do not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to IT support.

I will promote online safety and security with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access in line with the Online Safety Curriculum.

Appendix 3: Online Safety Training Needs – Self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student 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 students 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? Please record them here.	

Appendix 4: Online Safety Curriculum Overview

Online Safety Strand	Lifestyle & Health	The Social Web	Protecting Ourselves	Commercial Risks	News & Information
Foundation Stage	Sleep Choosing What to do online	Communicating Online Feeling Safe Online Personal Information	Online Friends		
Key Stage One	Screen Time Choosing What to do Online	Personal Information Being Kind Online Communicating Online	Online Strangers Feeling Uncomfortable Online Searching Safely	Passwords What is the Internet? Accepting Messages	Content Creators Scary News
Lower Key Stage Two	Screen Time Sleep Deciding what is appropriate	Friendship Online	Online Strangers Sharing Online	Advertising Personal Information Copyright Suspicious Messages Passwords	Digital Media Media Bias Verifying content and echo chambers

Online Safety Strand	Lifestyle & Health	The Social Web	Protecting Ourselves	Commercial Risks	News & Information
Upper Key Stage Two	Social Media Anxiety Self Esteem Inaccurate Health Information Digital 5-a-Day Online Stereotypes Game ratings Does the internet make us happy?	Control and Consent Social Media and Cyberbullying	Protecting our identity Protecting images of us online Unhealthy Attention Meeting online strangers	Internet advertisements and money on the internet Personal Information, Terms and Conditions In-app purchases and credit card information Recap Passwords	Analysing Digital Media Bias Fake News Verifying information online Echo Chambers
KS3	Gaming benefits and harms	Acceptable online behaviour Cyberbullying Online relationships	Grooming and exploitation via social media Nude image sharing The law and online behaviour	Gaming and the risk of gambling. Data protection and privacy Data usage Copyright and ownership e-commerce	The future and technology Fake news
KS4 & KS5	Impact of pornography on real life relationships Sexting Online influences.	Acceptable online behaviour Gaslighting Cyberbullying Freedom of speech.	Grooming and exploitation via social media Nude image sharing The law and online behaviour	Fraud, scam and phishing. Advertising Data protection and privacy Data usage	New Technologies – opportunities and risks.