Excalibur Academies Trust

Online Safety Policy

May Park Primary School

Date of approval	February 2021 (amended Nov 2022)
Approved by	CEO
Review date	February 2024

Registered Office: Excalibur Academies Trust, Granham Hill, Marlborough SN8 4AX
Registered in England and Wales
Company number: 8146633

Contents

1. Aims

Excalibur Academies Trust aims to :

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors, Board members and trustees,
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education (DfE) statutory safeguarding guidance, KCSIE and its advice for schools on :

- Teaching online safety in schools
- Preventing and tackling bullying and cyber bullying : advice for Principals and school staff
- Relationships and sex education (where applicable)
- Searching, screening and confiscation

It also refers to the Department'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 "good reason" to do so.

The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board and the individual schools governing board

The Trust Board has overall responsibility for all policies and will ensure that any amendments are made when legislation changes.

The Local Governing Body (LGB) of each school has an overall responsibility for monitoring policy and holding the Principal to account for its implementation.

The LGB 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).

The nominated Safeguarding governor is responsible for ensuring monitoring of online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Principal and senior leaders

The Principal is responsible for ensuring that staff understand the policy, and that it is being implemented consistently throughout the school.

- The Principal and another member of the leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made.

- The Principal and senior leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and disseminate knowledge.
- The Principal and senior leaders will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal online safety monitoring role.
- The senior leadership team will receive and review regular monitoring reports from the person responsible for online safety within the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school DSL and deputy/deputies are set out in our 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 Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and deal 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 Principal and/or governing board

This list is not intended to be exhaustive.

In some schools there will be an online safety co-ordinator who is not the DSL in these cases it is important that this person is line managed in this role by the DSL and the roles are clearly defined.

3.4 The ICT manager

It is acknowledged that in some schools the ICT manager is from the Trust central team or from an external organisation.

The ICT manager for May Park Primary School is Matt Evans and is part of Excalibur Academies.

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a termly 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 5) 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.

3.5 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 school's ICT systems and the internet (appendix 3) and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 Parents

Parents are expected to :

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

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

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

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, 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)

4. 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 :

From September 2020 all schools will have to teach:

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

This new requirement includes aspects about online safety.

Primary 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 only, including by pretending to be someone they are not.
- That the same principals 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The following relates to secondary schools and is for information only :

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, they 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 and 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

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 pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

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

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

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 one person or group by another person or group, where the relationship involves an imbalance of power (see also the school behaviour policy)

6.2 Preventing and address 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 a victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor 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 pupils, as part of safeguarding training (See section 11 for more details)

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 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.

6.3 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 pupils' 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 breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DFE's latest guidance on screening, searching and confiscation.

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, board members and governors are expected to accept an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 pupils, staff, volunteers, board members, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1,2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during :

- Lessons
- Clubs before or after school, or any other activities organised by the school

Mobile devices should be handed into the school office and collected at the end of the day. Any use of mobile devices in school by pupils 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

Staff members using a work device outside of 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 3.

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.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy and ICT and internet acceptable use agreement. 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 and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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.

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 meetings0.

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Trust and Education Scrutiny Committee. At school level it will be reviewed every year by the DSL and the review will be shared with the governing body.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Concerns and Complaints procedure
- ICT and internet acceptable use policy
- Excalibur Employment manual

Appendix 1 : EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil :
When I use the school's ICT systems (like computers & email) whether in school or at home and access the internet in school I will :

• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for schoolwork only
• I will 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 the pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.
Signed (parent/carer): **Date:**

Appendix 2 : KS2 to KS5 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
I will read and follow the rules in the acceptable use agreement policy **When I access the internet in school and use the school's ICT systems (like computers & email) whether in school or at home 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 username and passwords safe and not share these with others • Keep my private information 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 others • Always log off or shut down a computer when I'm 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 • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**
Signed (pupil) : **Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.
Signed (parent/carer): **Date:**

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

Adapt this agreement to reflect your school's approach, in line with any changes you make to this policy.

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 abide and follow the requirements set out in the Trust's IT acceptable use policy:

IT acceptable use policy

1. Introduction: This policy sets out the requirements with which you must comply when using the Trust's IT and when otherwise using IT in connection with your job including:
    1. The Trust's email and internet services.
    2. Telephones and faxes;
    3. the use of mobile technology on Trust premises or otherwise in the course of your employment (including 3G / 4G, Bluetooth and other wireless technologies) whether using an Academy, Trust or a personal device; and
    4. any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the Trust.
    5. This policy also applies to your use of IT off Trust premises if the use involves Personal Information of any member of the Trust community or where the culture or reputation of the Trust or any of its academies are put at risk.
2. **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the Trust's Disciplinary Procedure.
3. **Property:** You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to your line manager. You should not use the Trust's computers or other IT resources unless you are competent to do so and should ask for training if you need it.
4. **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not introduce or operate any hardware, software, code/script or data, additionally suspicious emails which have not first been checked by the Trust for viruses should not be opened
5. **Passwords:** Passwords should be long, for example you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:
    1. Your password should be difficult to guess, for example you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.
    2. You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.
    3. Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.
6. **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off or lock your device so that a password is required to gain access again
7. **Concerns**: You have a duty to report any concerns about the use of IT at the Trust to a senior colleague. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8. **Other policies**: This policy should be read alongside the following:
    1. Code of Conduct;
    2. data protection policy for Staff;
    3. information security policy; and
    4. acceptable use policy for pupils.

Internet

9. **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.
10. **Personal use:** The Trust permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust or it has been used for inappropriate purposes (as described in section 14 below) either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.
11. **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the Trust.
12. **Location services**: The use of location services represents a risk to the personal safety of those within the Trust community, the Trust's security and its reputation. The use of any website or application, whether on a Trust or personal device, with the capability of publicly identifying the user's location while on Trust premises or otherwise in the course of employment is strictly prohibited at all times.
13. **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the Trust or any of its Academies, without specific permission from the Principal. This applies both to "free" and paid for contracts, subscriptions and Apps.
14. **Retention periods**: The Trust keeps a record of staff browsing histories for a period of 30 days.

Email

15. **Personal use:** The Trust permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The Trust may monitor your use of the email system, please see paragraphs 26 to 30 below, and staff should advise those they communicate with that such emails may be monitored. If the Trust discovers that you have breached these requirements, disciplinary action may be taken.
16. **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.
17. **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18. **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.
19. **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the Trust's IT system to suffer delays and / or damage or could cause offence.
20. **Contracts:** Contractual commitments via an email correspondence are not allowed without prior authorisation of the Principal.
21. **Disclaimer:** All correspondence by email should contain the Trust's disclaimer.
22. **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). Staff must be aware that anything they put in an email is potentially disclosable**.**

Monitoring

23. The Trust regularly monitors and accesses its IT system for purposes connected with the operation of the Trust. The Trust IT system includes any hardware, software, email account, computer, device or telephone provided by the Trust or used for Trust business. The Trust may also monitor staff use of the Trust telephone system and voicemail messages. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).
24. The purposes of such monitoring and accessing include:
    1. to help the Trust with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and
    2. to check staff compliance with the Trust's policies and procedures and to help the Trust fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.
25. Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.
26. The Trust also uses software which automatically monitors the Trust IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).
27. The monitoring is carried out by The Trusts IT personal or a company contracted to provide the Trust with ICT services and support. If anything of concern is revealed as a result of such monitoring then this information may be shared with the schools Principal and other senior staff where necessary and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

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 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 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: online safety training needs – self audit for staff

The following questions will be shared with Staff via Microsoft Forms

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?	
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 5 :ONLINE SAFETY INCIDENT REPORT LOG

To be used by schools who do not have CPOMS or Bromcom for recording safeguarding incidents.

Only to be used if online systems are unavailable.

ONLINE SAFEY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**