Bacton Primary School · Cedars Park Primary School · Mendlesham Primary School · Stowupland High School · The John Milton Sixth Form AT STOWUPLAND HIGH SCHOOL

JOHN MILTON
ACADEMY TRUST
Ambition • Aspiration • Excellence

Online Safety Policy

JMAT 042

History of Document:

Issue No	Author/ Owner	Date Written	Reviewed by Trust on	Comments
V.1	CEO	August 2023	5-Sep-23	JMAT 042 replaces the E-Safety Policy

Contents

1. Aims

1.1 Our Trust aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and those in governance
- Identify and support groups of learners that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 Categories of risk

Our approach to online safety is based on addressing the following 4 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

2. 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 learners' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 Governance

These roles are reflected in the Trust's Scheme of Delegation which is reviewed annually.

3.1.1 Trust Board

The Trust Board has overall responsibility for approving and monitoring this policy and holding schools to account for its implementation through the Local Improvement Boards.

The Trust Board must ensure that all schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness through the Trust's ICT tem.

The Trust Board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

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

3.1.2 The Local Improvement Board

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

The Local Improvement board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. In practice, this operates through the Trust's Safeguarding Task Group, chaired by an Executive Headteacher.

The Local Improvement Board designated safeguarding member will meet with appropriate staff to discuss online safety and monitor online safety data as provided by the designated safeguarding lead (DSL) through the termly School Improvement Report and the regular Safeguarding Report.

3.1.3 All those in governance will:

- Ensure they have read and understand this policy (via GovernorHub)
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix D)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some learners 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

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of each school’s designated safeguarding lead (DSL) and deputies are set out in the Local Procedures for each school.

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 and Trust personnel to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT network manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT network 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 safeguarding and child protection policy
- Ensuring that any online safety incidents are logged (see appendix F) 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’s behaviour policy
- Updating and delivering staff training on online safety (see appendix E)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and Local Improvement Board through the
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The ICT network manager

The ICT network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school’s ICT systems on a monthly 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 F) 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

(see also Appendix H)

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 D), and ensuring that learners follow the school's terms on acceptable use (appendices B and C)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the DSL **and** the Network Manager
- Following the correct procedures by submitting a request to a Senior Leader or Subject Leader, who will then make a request to IT support, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix F) 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
- 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.

3.6 Parents/carers

Parents/carers are expected to:

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

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

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

4. Educating learners about online safety

Learners will be taught about online safety as part of the school curriculum. At primary, this will include: Relationships education and health education and at secondary, it will include: Relationships and sex education and health education

Primary curriculum:

In **Key Stage 1**, learners 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

Learners 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**, learners 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

Secondary curriculum:

In **Key Stage 3**, learners 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

Learners 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**, learners 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 that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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 learners with SEND.

5. Educating parents/carers about online safety

Each school will raise parents/carers' awareness of internet safety in news, bulletins and other communications home, and also in information on school websites This policy will also be shared with parents/carers.

The school will let parents/carers 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/carers 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 or the headteacher.

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 school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners 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 learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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

All staff, those in governance and volunteers (where appropriate) will receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

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 learners, 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 (as set out in the behaviour policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners, 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 learners and staff. If the search is not urgent, they will seek advice from the DSL or the most senior member of staff on site
- 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 co-operation

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 DSL and 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/carer 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 learners 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 behaviour policy - searches and confiscation section

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

7. Acceptable use of the internet in school

All learners, parents/carers, staff, volunteers and those in governance are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices B to D). 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.

The websites visited by students, staff, volunteers, those in governance and visitors (where relevant) will be monitored to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices B to D.

8. Student use of mobile devices in school (secondary phase)

8.1 Mobile Phones

At the secondary phase, students may bring mobile devices into school, but are not permitted to use them during:

- Lessons (unless directed and monitored by a teacher)
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Social times (inside the school)

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices B and C).

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.

8.2 Laptops and Tablets

The school understands that personal laptops or tablets can be a very important tools to facilitate learning, particularly for post-16 learners. In order to simplify the process, the school will provide a single one time connection. Once connected, students will be able to access Google Workspace, Show my Homework and other Internet based learning platforms.

Please note that all iInternet access is monitored on all devices (including personal devices) that use the school Wi-Fi network.

The first time students want to connect a laptop or tablet to the BYOD network, they will need to speak to the Sixth Form Administrative Assistant to access the Wi-Fi code. Any personal device must be running Windows 10 or 11, Chrome OS, Mac OS 11 onwards, IOS 16 onwards or Android 11 onwards and have an up to date antivirus program installed and running.

The IT team can provide basic assistance with getting a device connected to the network bu unfortunately cannot offer any other support for personal devices.

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

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

Work devices must be used solely for work activities.

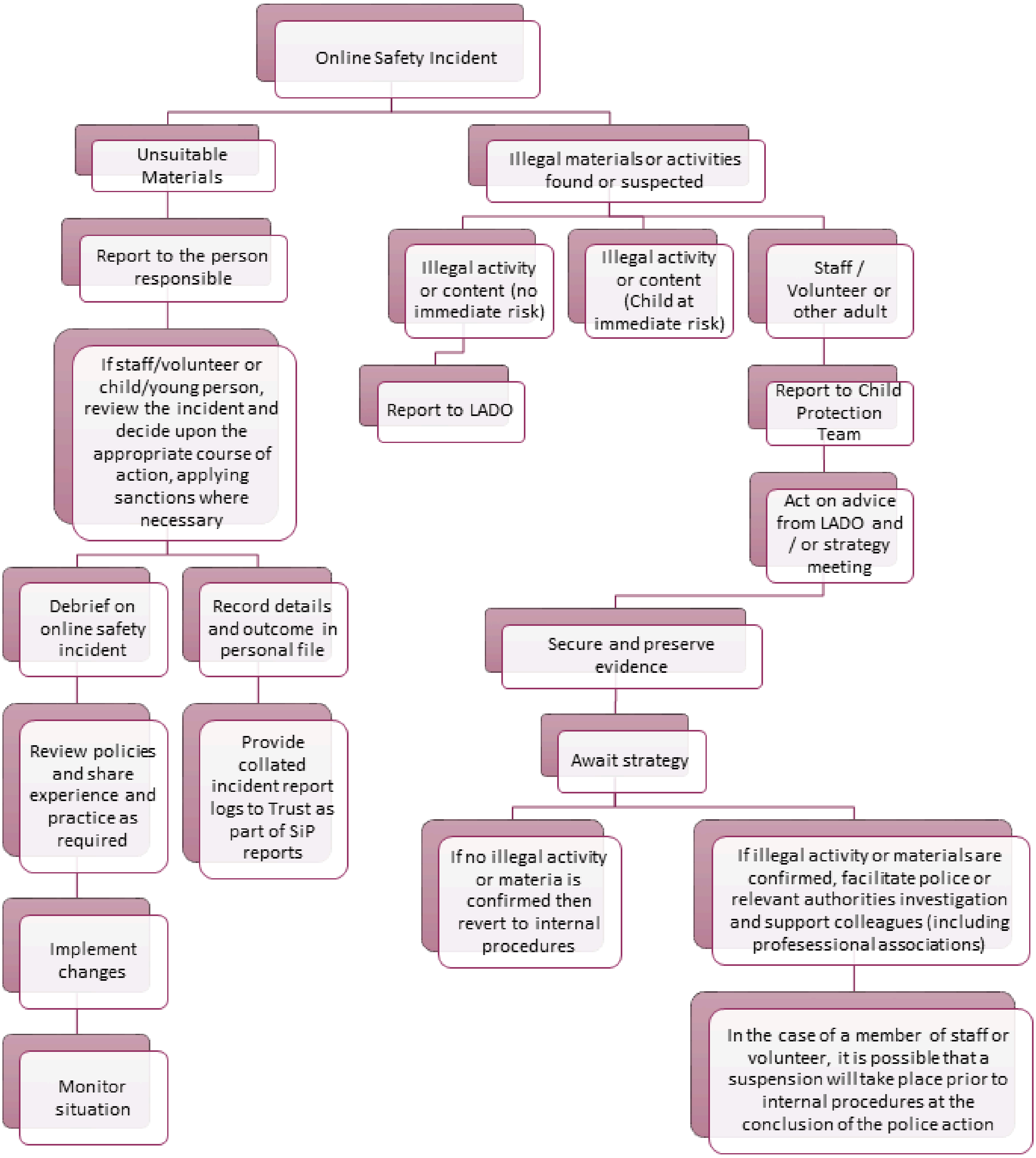
If staff have any concerns over the security of their device, they must seek advice from the Trust's network manager.

10. How the school will respond to incidents of misuse

Where a pupil misuses the school's ICT systems or internet, each school will follow the procedures set out in the relevant policies on behaviour and ICT and internet acceptable use. 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.

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


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible
Illegal activity or content (no immediate risk)
Illegal activity or content (Child at immediate risk)
Staff / Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to LADO
Report to Child Protection Team
Act on advice from LADO and / or strategy meeting
Debrief on online safety incident
Record details and outcome in personal file
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to Trust as part of SiP reports
Await strategy
If no illegal activity or materia is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, facilitate police or relevant authorities investigation and support colleagues (including professesional associations)
Implement changes
In the case of a member of staff or volunteer, it is possible that a suspension will take place prior to internal procedures at the conclusion of the police action
Monitor situation

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 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 learners can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term

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

Trustees and Local Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety through CPOMS. A specific incident report log can be found in appendix F.

This policy will be reviewed every year by the Trust's Safeguarding Lead, working with other executive personnel. At every review, the policy will be shared with the Trust Board and Local Improvement Boards. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks learners face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and child protection policy
- Local Procedures for Safeguarding and Child Protection
- Behaviour policy (individual to each school)
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy (for staff and for students)
- Curriculum Policies (eg PSHE/RSE)

Appendix A:

Promoting online-safety through the curriculum

Bacton and Mendlesham

1. Year Group content and delivery

In Key Stage 1, the Teach Computing Curriculum covers the objective: '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' in the following units of work:

Year 1	Data and information – Grouping data Creating media – Digital writing
Year 2	Computing systems and networks – IT around us Creating media – Digital photography Data and information – Pictograms

In Key Stage 2, the Teach Computing Curriculum covers the objective: 'use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact' in the following units of work:

Year 3	Creating Media – Stop Frame animation
Year 4	Computing Systems and Networks – The Internet Creating Media – Audio Creating Media – Photo Editing
Year 5	Creating Media – Video Production
Year 6	Computing systems and networks - Communication and collaboration Creating media – Web page creation Creating media – 3D Modelling

For PSHE, Jigsaw is followed across the school. By the end of a child's primary education they should know:

Online relationships

(R20) that people sometimes behave differently online, including by pretending to be someone they are not

(R21) 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

(R22) the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

(R23) how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.

(R24) how information and data is shared and used online.

(R25) what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

(R32) where to get advice e.g. family, school and/or other sources.

Internet safety and harms

(H11) that for most people the internet is an integral part of life and has many benefits

(H12) about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical well-being

(H13) how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private

(H14) why social media, some computer games and online gaming, for example, are age restricted

(H15) that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health

(H16) how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted

(H17) where and how to report concerns and get support with issues online.

Additional Advice and Guidance:

Each year the school takes part in Safer Internet Day. We also aim to have Digital Leaders to promote online safety in school on a peer to peer basis.

Promoting online-safety through the curriculum

Cedars Park

1. Year Group content and delivery

Year 1:

- Know how to log in safely.
- Know how to navigate to a document area where saved work by child can be found.
- Know how to use search to locate applications or resources on a platform such as Purple Mash.
- Know how to enhance work by adding multimodal items such as text and images.
- Know how to open, save and print work.
- Know the importance of logging out of an account

Year 2:

- Know how searches can be refined when searching digitally and therefore attempts refining when searching.
- Know that digitally created work can be shared with others e.g. Purple Mash Display Boards.
- Has knowledge and understanding about sharing more globally on the Internet.
- Know that email is a type of communication tool.
- Know how to open and send simple online communications in the form of email e.g. 2Email (virtual email client).
- Know that there is an appropriate way to communicate with others in an online situation.
- Know that information put online leaves a digital footprint.
- Know some steps that can be taken to keep personal data and hardware secure.

Year 3:

- Know what makes a safe password and how to keep it safe.
- Know the main outcomes of not keeping passwords safe.
- Know all the common ways the Internet enables people to effectively communicate.
- Know that a blog can be used to help communicate with a wider audience.
- Know how to contribute to a blog with clear and appropriate messages.

- Know that some information held on websites may not be accurate or true.
- Beginning to know how to search the Internet and how to think critically about the results returned.
- Know why there are age restrictions on digital media and devices.
- Know where to turn to for help if they see inappropriate content or have inappropriate contact from others.

Year 4:

- Know that information put online leaves a digital footprint or trail and can expand on prior years' scope of this fact.
- Know some of the ways children can protect themselves from online identity theft.
- Know that information put online by users could be used for identity theft.
- Know the main risks and benefits of installing software and applications.
- Know that copying work of others and presenting it as their own is plagiarism.
- Knows the consequences of plagiarism.
- Knows appropriate behaviour when participating or contributing to collaborative online projects for learning.
- Know some of the main positive and negative influences technology has on health and the environment.
- Knows the importance of balancing screen time with non-screen time.

Year 5:

- Know in more detail from prior learning of the impact that sharing digital content can have.
- Know how to think critically about information they share online.
- Know responsibilities they have for themselves and others regarding online behaviour.
- Know and have developed knowledge from prior years about maintaining secure passwords.
- Know about image manipulation using software and the advantages or disadvantages of this when shared online. Know what is meant by appropriate and inappropriate text, photographs and videos.
- Know about the impact of sharing media such as photographs and videos online.
- Know about the importance of citing content online from others and know how to do this.
- Know how to select keywords and search techniques to find relevant information to increase reliability.

Year 6:

- Know the benefits and risks of mobile devices broadcasting the location of the user/device, e.g., apps accessing location.
- Know what secure sites are.
- Know that secure sites will have industry standard seals of approval.
- Build on knowledge of Digital Footprints. For example, know how and why people use their information.
- Build on knowledge of appropriate online behaviours and how this can protect themselves and others from possible online dangers. For example, the dangers of promoting inappropriate content online.
- Have greater knowledge of how to make more informed choices of how free time is used.
- Know the effects on individual health when having too much screen time.

2. Additional advice and guidance

At Cedars Park Primary, we are signed up to the National Online Safety website which provides school with updated information on safeguarding and contextual issues around the latest online games and safety concerns.

In addition, school regularly share factsheets and information with parents produced by NOS to keep them up to date on how best to support their children with keeping safe online.

Promoting online-safety through the curriculum

Stowupland High School

1. Year group content and delivery

Year Group	PSHE	ICT/Computing
7	Online friendships Cyberbullying Body image and the internet	Cyber explorers ICT
8	Digital and media literacy	Cyber bullying Social media Sexting Fake News
9	Radicalisation and internet grooming Online gambling	Cyber security
10	Body image and the internet Online gambling Anti fraud education	
11	Online presence and reputation	

2. Additional advice and guidance

- E-safety tips for parents/carers on weekly newsletter
- E-safety display
- Take part in Safer Internet Day
- Annual parent/carer workshop
- Assemblies throughout the year for children
- All children to sign Code of Conduct

Appendix B: EYFS and KS1 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of learner:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I 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 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 learners using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix C: KS2, KS3 and KS4 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of learner:

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 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 learners 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 D:

Acceptable use agreement (staff, those in governance, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, THOSE IN GOVERNANCE, VOLUNTEERS AND VISITORS

Name of staff member/trustee/local board member/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 learners without checking with teachers first
- Share confidential information about the school, its learners or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Use for personal financial gain, gambling, political purposes or advertising
- 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 will ensure that my use of the internet, and any work device will be in line with the Acceptable use of ICT Policy, the Online Safety Policy and the Staff Code of Conduct.

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 learners in my care do so too.

Signed (staff member/trustee/local board member/volunteer/visitor):	**Date:**

JOHN MILTON
ACADEMY TRUST
Ambition • Aspiration • Excellence

Appendix E: Online safety training needs – self-audit for staff

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 learners 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, those in governance and visitors?	
Are you familiar with the school's acceptable use agreement for learners and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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 F: 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**

Appendix G:

Online-Safety Investigation Form

Investigation Type	Complaint	
	Incident of Computer / Internet Misuse	
	Incident of mobile phone misuse	
	Other	
Date first alerted		
Name / Role of Investigator		
For Computer Misuse Only Name/ Role of Investigator		
Complaint Only Contact details of complainant		
Summary of Issue(s)		
Investigation: *Please provide as much detail as possible including evidence collected or not collected, persons interviewed or not interviewed, anonymized statements, third parties, witnesses etc. Please reference any documentary or other evidence.*		
Computer Misuse Only: *Name, Serial Number and location of device identified as misused*		
Computer Misuse Only: *Name, Serial Number and location of device used for review*		

Findings:			
Recommendations:			
Investigator's signature:		**Date:**	
Supporting documents *List all documents collected as part of investigation and included in report.*			
File location:	*List file path or filing location where documents pertaining to Investigation will be held. Complaints must be held for six years from the date of resolution and then reviewed for further retention in cases of contentious disputes. Retention for cases of Incident Misuse will be as per pupil records then reviewed for further retention in cases of criminal or serious cases.*		
REVIEW AND SIGN OFF			
Name:		**Role:**	
Signed:		**Date:**	

Appendix H: ICT Infrastructure, Equipment, Filtering and Monitoring

G.1 Schools within the John Milton Academy Trust are responsible for ensuring that school infrastructure is safe and secure and that procedures within this policy are implemented. The management of technical security is the responsibility of the Trust's Network Manager.

G.2 The school and Trust ICT Team will ensure that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the Trust's Data Protection and FOI policy
- logs are maintained of access by users and of their actions while using the system (e.g. via Smoothwall, inadvertent or deliberate access of unauthorised systems or data)
- there is effective guidance and training for users
- there are annual reviews and audits of the safety and security of school computer system (as identified in sections 1 and 2)
- there is oversight from senior leaders, and that this monitoring has an impact on policy and practice.

G.3 Appropriate security measures are in place through the Antivirus/ Malware protection to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.

G.4 The Trust's Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. A record of licences should be maintained.

G.5 All users will have clearly defined access rights to school technical systems**.** Guest temporary access onto the school's internet will be via dedicated Guest profiles. Access to specific school systems will be by agreement of the school's leadership. Audits of network, Office365 / Google Classroom IDs be undertaken annually by the Trust's ICT team to ensure appropriate access rights are in place.

G.6 A safe and secure username/password system will apply to all school technical systems, including networks, devices, email. The Online-safety Lead, together with the Data Protection Lead is responsible for regular audits or registered users for all key systems.

G.7 Internet access is filtered for all users. Illegal content must be filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists must be regularly updated, and internet use must be logged and regularly monitored. Requests for filtering changes must be agreed by the E-Safety Lead or DSL. IT staff must keep a log of such requests (this may be within the filtering system).

G.8 The school may monitor and record the activity of users on the school systems.

G.9 Staff who have responsibility for multiple school systems, including IT staff and Administrators, must log user IDs and passwords in a password protected document in Office365/ GSuite to support disaster recovery. Passwords must not be written down.