Online Safety Policy

Online safety is an integral part of safeguarding. This policy sets out our approach to online safety to empower, protect and educate learners and colleagues in their use of technology. It establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate

Version number	4.0
Consultation groups	Central Executive Team, Blended learning network, IT technicians and Headteachers
Approved by	Board of Trustees
Approval date	September 2025
Adopted by	Advisory Board
Adopted date	September 2025
Policy/document owner	Trust Online Safety Lead
Status	Statutory
Frequency of review	Annual
Next review date	September 2026
Applicable to	Discovery Trust All schools

Document History

Version	Version Date	Author	Summary of Changes
V1.0	9th September 2021	Adam Lapidge – Online Safety Lead	*New policy prepared in line with:* ▪ *Keeping children safe in education -September 2021* ▪ *Working Together to Safeguard Children", 2018* ▪ *Ofsteds Review of Sexual Abuse and Colleges – June 2021*
V2.0	6th September 2023	Adam Lapidge – Online Safety Lead	*Updated policy in-line with:* ▪ *Keeping children safe in education – September 2023* ▪ *Dfe filtering and monitoring standards*
V3.0	16th August 2024	Adam Lapidge – Online Safety Lead	*Updated policy:* ▪ *Updated wording for curriculum to fit all schools.* ▪ *Updated annex 1: Technical Systems* ▪ *Updated linked policies to include AI* ▪ *AI subsection added*
V4.0	29th August 2025	Adam Lapidge – Online Safety Lead	*Updated policy:* ▪ *Removed 'staff' and replaced with 'colleague' throughout document.* ▪ *Updated section on mobile devices* ▪ *Updated section on AI* ▪ *Updated section on Pupil smart watches* ▪ *Added section on Digital Wellbeing*

Contents

1. Statement of Intent

The online safety policy is intended to demonstrate the organisation's commitment to:

- Ensuring the safety and wellbeing of children, young people and adults is paramount when using the internet, social media or mobile devices.
- Providing colleagues and volunteers with the overarching principles that guide our approach to online safety.
- Ensuring that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of Discovery Trust including colleagues, students, advisory board members, volunteers, parents, carers, visitors, and community users who have access to and are users of Trust digital technology systems, both in and out of the Trust.

2. Linked policies

This policy statement should be read alongside our organisational policies and procedures, including:

- Acceptable Use policy (KS1 & KS2)
- Anti-Bullying Policy (including Cyberbullying)
- Document Retention Management Policy
- GDPR Data Protection Strategy
- Mental Health and Wellbeing Policy
- Mobile Phone and Smart technology policy (linked 11.2)
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Student Behaviour Policy
- Social Media Policy
- Special Educational Needs and Disability Policy
- Home Learning Protocol Policy
- AI Governance Guidance

Colleague related Policies and Procedures:

- Acceptable Use policy
- Disciplinary Policy and Procedure
- Mobile Phone and Loaned Property Policy
- Staff handbook which includes Staff Code of Conduct
- Staff Wellbeing Policy
- Trust Platform Working document

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for online safety.

3. Key Roles and Responsibilities

We take a whole-school approach to online safety, and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all colleagues and volunteers will read and understand this policy and implement it consistently.

3.1 Governance

Trustees and Advisory Board Members and play an important part in monitoring the online safety provision across the trust and within schools. They have a responsibility to keep up to date with online safety by receiving appropriate online safety training (delivered by Trust Online Safety Lead).

The Trust Board is responsible for:

- Reviewing and approving this policy.
- Monitoring the effectiveness of the policy at a Trust level by reviewing data and reports from the Trust Online Safety Lead and Trust Safeguarding Lead.
- Appointing a designated Trustee with oversight of safeguarding and online safety at a trust level. It is the role of the lead trustee to meet with the Trust Safeguarding Lead regularly to ensure any weaknesses are addressed.
- Agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in schools and across the Trust.

The school Advisory Board is responsible for:

- Adopting this policy locally ensuring it meets the needs of the school.
- Monitoring the effectiveness of the policy at a school level by monitoring data and audit reports for the Trust Online Safety Lead and Trust Safeguarding Lead.
- Appointing a designated Advisory Board Member with oversight of safeguarding and online safety at a school level. It is the role of the lead Advisory Board Member to meet with the school Safeguarding Lead regularly to ensure any weaknesses are addressed.
- Ensuring that schools are meeting the DFE filtering and monitoring requirements and a nominated member oversees its implementation.
- Agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in school.

3.2 Trust Online Safety Lead

The role of Online Safety lead forms part of the Trust's safeguarding team. The Trust Online Safety Lead will receive regular training on online safety and be aware of the potential for serious child protection and/or safeguarding issues that may arise from the online world. They will have overall oversight of the trust's online safety strategy. Key responsibilities:

- Delivering training trust-wide to school online safety DSLs
- Monitoring online safety in schools through yearly audits*
- Ensuring support mechanisms are in place for schools dealing with complex situations.
- Regularly updating trust leaders on the progress made with online safety, as well as reporting data to the trust board.
- Ensuring that there are robust protocols in place for both monitoring and reporting online safety issues.
- Ensuring all colleagues adhere to the policies and procedures around online safety. E.g. acceptable use policies and loan equipment agreements.
- Responsible for actioning the annual review of the online safety policy.

*The Trust Online Safety Lead will use the SWGFL 360 Safe audit as part of its yearly online safety audit with the expectation that all trust schools move towards obtaining the Online Safety Mark Certification. Details of this can be found here: https://swgfl.org.uk/products/360-degree-safe/
The purpose of these audits is to ensure the school continues to:

- Review and develop its online safety strategy.
- To find and action any areas of development within the school online safety program.

3.3 Head Teachers/Head of Schools and SLT

Head teachers / Head of school and members of SLT take overall responsibility in ensuring that all Colleagues and students understand and follow the policies and procedures of online safety.

Key responsibilities:

- To liaise with the Online Safety DSL about the development of the school's online safety strategy.
- Support the Online Safety DSL in carrying out their role.
- Review the online safety curriculum with the Online Safety DSL.
- Share the online safety audit report and actions to the Advisory Board.
- To know the procedures in the event of serious online safety allegations against a colleague.
- Responsible for ensuring the Online Safety Lead is given time to receive suitable training to support them in their role.
- Ensure all colleagues understand this policy and that it's implemented consistently.
- Reviews the school's infrastructure/network with the Chief Technical Officer or Phase IT Lead to ensure it is safe and fit for purpose.

3.4 School Online Safety Lead

This role will be part of the school's Designated Safeguarding Lead team. The Online Safety DSL will be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues. Key responsibilities:

- Responsibility for online safety issues in school.
- Liaise with Trust Online Safety Lead on the school's online safety development and strategy.
- Liaise with external agencies where necessary.
- Provide regular reports on online safety in school to the headteacher/head of school.
- Keep up to date with current legislation, developments, and resources.
- Provide training and advice for all colleagues across school.
- Lead role in personalising policies/documents.
- Attends any relevant meetings with Advisory Board members and updates them on progress of online safety.
- Ensure student voice is considered as part of online safety development/strategy.
- Liaise with the Trust in the event of serious incidents.
- Ensure all online safety incidents are logged onto CPOMs, providing training for staff where necessary.

3.5 School IT Team

School IT technicians are the first line of defense against online safety, and they play a huge role in ensuring that students and colleagues are kept safe. Key responsibilities are to:

- Ensure that school networks are secure and safe to use.
- Regularly monitor school networks and internet.
- implement and update monitoring software/systems are as requested by Trust's senior technical team.
- Ensure that only authorised users can access the network, and these users adhere to the trust's password policy.
- Ensure that they keep up to date with relevant online safety updates.
- Ensure that filtering policies are applied to the correct users.
- Ensure that any filtering request changes are liaised and agreed with head teachers / SLT before actioning.
- Ensure that any online safety incidents are sent to class teachers and SLT for actioning.
- Management of Office365 and ensuring policies and procedures are being followed.

3.6 Teaching and Support Staff

Teachers and support colleagues are the day-to-day contact for students and therefore responsible for promoting safe online safety behaviour. Key responsibilities are to:

- Ensure they attend any relevant training that is issued by the headteacher, PedTech Lead or Online Safety DSL.
- Ensure that they adhere to the policies and procedures relating to online safety. E.g., acceptable use policy, loan agreement form, staff handbook.

- Support students understanding and ensure they follow online safety procedures and policies.
- Ensure that where there is pre-planned internet use, students are guided to sites that are suitable.
- Report any online safety concerns to the online safety DSL.
- Ensure policies around mobile phones are enforced with all students.
- Ensure digital communications with students/parents/carers on carried out using official school systems and that conversations always remain professional.
- Ensure they deliver the online safety curriculum to all students.
- Ensure online safety issues are embedded into all aspects of the curriculum.

3.7 Students

Students are responsible for:

- Ensuring that they use the digital technology systems in accordance with the student acceptable use policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate material.
- Adhering to the school mobile phone policies and are aware of the consequences if they don't follow this.
- Understanding the need for good online safety behaviour both in and out of school.
- Providing valuable feedback about online safety through surveys and discussions.

3.8 Parents/carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school websites, social media, and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Online learning platforms (Microsoft Teams) by following the Home Learning Protocol Policy.
- Their children's personal devices in the school/academy (where this is allowed).

3.9 Community Users

Community users who have access to the school systems or programmes as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy/Agreement before being provided with access to school systems. This will be done as they enter the building using our signing in system.

4. Managing online safety

All colleagues will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Online Safety Designated Safeguarding Lead has overall responsibility for the school's approach to online safety, with support from the school's senior leadership team, and will ensure that there are strong processes in place to handle any concerns about students' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Colleagues receive regular training.
- Colleagues receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted termly on the topic of remaining safe online.

5. Online safety in the curriculum

We want our students to take responsibility and act in a responsible way.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Student's will be taught about online safety as part of the curriculum

All schools have to teach:

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

In **Key Stage (KS) 1**, students 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

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

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

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

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The 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 students with SEND.

5.1 Digital Wellbeing

At Discovery Trust, we recognise that digital wellbeing is a vital component of safeguarding and online safety. As technology becomes increasingly embedded in students' lives, it is essential to promote healthy, balanced, and responsible use of digital devices and online platforms.

Objectives

Our digital wellbeing strategy aims to:

- Encourage students to develop healthy habits around screen time and device use.
- Promote positive online behaviours and respectful digital interactions.
- Raise awareness of the impact of technology on mental health and emotional wellbeing.
- Support students in managing online pressures, including social media, gaming, and digital communication.

Curriculum Integration

Digital wellbeing is embedded across the curriculum and includes:

- Discussions on screen time, sleep hygiene, and digital balance.
- Lessons on managing online stress, peer pressure, and social comparison.
- Activities that promote self-regulation, mindfulness, and critical thinking in digital contexts.
- Opportunities for students to reflect on their digital habits and make informed choices.

Student Empowerment

Students are encouraged to:

- Take regular breaks from screens and engage in offline activities.

- Use technology purposefully and mindfully.
- Seek help if they feel overwhelmed or negatively affected by online interactions.
- Participate in wellbeing surveys and discussions to shape the school's digital wellbeing approach.

Parent Engagement

We work closely with parents and carers to:

- Share guidance on managing screen time and promoting digital wellbeing at home.
- Provide resources and workshops on topics such as social media use, gaming, and online pressures.
- Encourage open dialogue between families and children about digital habits and mental health.

6. Parent awareness and working with the wider community

We understand that many parents and carers only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of children's online behaviour. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will provide information and awareness to parents and carers through:

- Curriculum activities, themed online safety awareness weeks. High profile events/campaigns e.g Safer Internet Day and Wellbeing Week.
- Letters, school newsletters, school web site
- Discovery Live - Webinars
- Parent/carers evenings
- Parent workshops
- Online Safety assemblies

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

All parents sign an acceptable use policy on behalf of their children when they join the school and then re-sign annually. (**Appendix 1)**

7. Training

7.1 Colleagues

It is essential that all colleagues receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training is made available to colleagues. This will be regularly updated and reinforced. An audit of the online safety training needs of all colleagues will be carried out regularly.
- All new colleagues receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events or as part of internal training from the Trust's Online Safety Lead.
- This Online Safety policy and its updates will be presented to and discussed by colleagues in staff/team meetings/training sessions.
- Colleagues are expected to read and understand the trust's platform working document which outlines the safe use of applications and platforms with students.

7.2 Trust Online Safety Lead DSL

It is essential that the Trust Online Safety Lead DSL receives additional training to support them in their role. This training will be done by:

- Attending advanced online safety training DSL training on an annual basis.
- Participating in online safety expert groups (SWGfL 360 Safe Assessor Programme).
- Attending expert external training sessions through various providers.
- Keeping up to date with latest legislation and policy changes.

7.3 Trustees and Advisory board members

Advisory Board members/trustees take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This will be offered through:

- Participation in Trust training sessions delivered by the Online Safety Lead.

8. Online safety concerns

8.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

Cyberbullying against students or colleauges is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

8.2 Child on child abuse

Students may use the internet and technology as a vehicle for sexual abuse and harassment. The following are examples of online harmful sexual behaviour of which colleagues 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

The school will respond to all concerns regarding online peer-on-peer sexual abuse and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

8.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Colleagues will be aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Students are less likely to report grooming behaviour because:

- The student believes they are talking to another child
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.

- The student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

8.4 Child sexual exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CSE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where colleagues have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

8.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

8.6 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 about 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.

8.7 Artificial Intelligence

Artificial Intelligence (AI) tools are now widely accessible and increasingly integrated into everyday life. Students, staff colleagues, and parents/carers may be familiar with generative AI platforms such as ChatGPT, Google Gemini, and others, which can produce text, images, audio, and video content. While these tools offer significant educational benefits, they also present new risks that must be carefully managed.

Educational Use of AI

Discovery recognises the potential of AI to enhance learning, creativity, and problem-solving. We encourage the responsible use of AI tools to support educational outcomes, provided they align with our safeguarding, data protection, and ethical standards.

Risks and Misuse of AI

AI technologies can also be misused in ways that cause harm, distress, or reputational damage. Examples include:

- **Deepfakes**: AI-generated images, audio, or videos that falsely depict individuals, including deepfake pornography or hoaxes.
- **AI-assisted bullying**: Using AI to create harmful content, impersonate others, or spread misinformation.
- **Plagiarism and academic dishonesty**: Using AI to generate work without proper attribution or understanding.
- **Data exploitation**: Many AI systems collect and process large volumes of personal data, which may compromise the privacy of students and staff.

Any use of AI to harass, intimidate, or harm others will be treated seriously and addressed in accordance with our Behaviour Policy and Safeguarding procedures.

Staff Responsibilities

Staff colleagues must remain vigilant when introducing or using AI tools within the school or trust. Key responsibilities include:

- **Risk Assessment**: Before deploying any new AI tool, staff must conduct a risk assessment to evaluate its safety, data handling practices, and potential impact on students.
- **Data Protection Compliance**: AI tools must comply with UK GDPR and internal data governance policies. Staff should avoid using tools that store or process student data without clear consent and robust safeguards.

- **Monitoring and Guidance**: Staff should actively monitor student use of AI tools and provide guidance on ethical and safe usage.

Student Awareness and Education

We are committed to educating students about the responsible use of AI. This includes:

- Understanding how AI works and its limitations.
- Recognising and reporting harmful or misleading AI-generated content.
- Respecting others' privacy and digital rights when using AI tools.

Discovery Trust will ensure:

- Robust safeguards are in place before introducing new AI systems.
- Student personal data is never input into open AI systems.
- Provide clear guidance for colleagues on using approved AI systems effectively and safely.
- Filtering systems are in place and effective in blocking unwanted AI systems.

Colleagues at Discovery Trust will always ensure they conduct a risk assessment before using any AI system that isn't on the approved list. It is their responsibility to make sure that the platforms they use do not put students or other colleagues at risk. Colleagues should familiarise themselves with the Trust AI guidance policy to understand the Trust expectations.

9. Responding to online incidents

9.1 Responding to student incidents

Where a student misuses the school's IT 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.

The schools DSLs will determine the seriousness of all incidents and report all illegal activities/incidents to the appropriate organisation, these include:

- Police
- CEOP (child exploitation and online protection)
- CyberChoices
- Social workers

- Health professionals

9.2 Responding to staff incidents

Where a colleague misuses the school's IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. 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, or otherwise serious incidents, should be reported to the police. A flow chart in dealing with illegal activity (**appendix 2)** supports the school in taking the correct action.

10. Personal devices

10.1 Students

Students in Year 5 and 6 may bring mobile devices into school. Parents/Carers will need to complete an agreement that their child can bring a mobile phone into school. Students must hand their mobile device into the locked box (via the class teacher) where it will be kept securely. Students are not allowed to use their mobile phone during the school day, this includes:

- Lessons
- Playtime/Lunchtime
- Clubs before or after school

Any breach of the mobile device agreement may trigger disciplinary action in line with the school behaviour policy and could result in confiscation of their device.

10.2 Colleagues

Colleagues must not use a personal device (e.g., phones and tablets) throughout the school day, unless this is in their own break/lunch time. Colleagues are not permitted to take or store images of students on their mobile device. Personal information about colleagues, students, or the school is not to be stored on any personal device.

Personal mobile phones must not be used to contact students or parents. During school outings nominated colleagues will have access to a school mobile phone which can be used for emergency or contact purposes.

11. Technical Systems

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that internet filtering is actively monitored for misuse. A full description of our policies are procedures relating to our technical systems can be found in Annex 1: Technical Systems

11.1 Filtering and Monitoring

Discovery trust recognises that filtering and monitoring plays a huge role in safeguarding it's students and has accessed it's systems against the Dfe's latest filtering and monitoring standards (https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges). The school has reviewed these filtering and monitoring standards to ensure the specifications have been met. This includes:

- Ensuring a member of senior leadership and governor is responsible for ensuring standards are met.
- The IT team has technical responsibility for ensuring filtering and monitoring meets the standard. The trust online safety lead will oversee the technical team on this.
- The school reviews it's filtering system regularly and has checked that they are a member of IWF, CTIRU and is blocking illegal content including child abuse material (CSAM). Termly reports are compiled and sent to Trust Online Safety Lead.
- The school reviews it's monitoring system regularly to ensure that it is effective in safeguarding its students.

11.2 Smart and Mobile Technology

The school understands that the rapid development of smart and mobile technology possesses an on-going online safety risk to students. The development of mobile devices and smart watches has meant that students are 'online' 24 hours a day. The school is committed to ensuring that we have procedures and systems in place when dealing with Mobile and Smart Technology in an ever change digital environment. Please see Annex 2: Mobile and art Technology for more information about how we manage our mobile and smart devices.

12. Remote learning

All remote learning is delivered in line with the school's Home Learning Protocol Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, monitoring software installed, has working audio and video and can download documents where appropriate. The school is not responsible for ensuring that devices that go home have strict filtering installed and this is the responsibility of the parent/carer to ensure safe use.

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 colleagues 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 and filtering, on devices not owned by the school.

12. Policy review

This policy will be reviewed by the Trust Online Safety Lead annually and updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. A formal review will be completed every two years for Trust Board approval.

Appendix 1: Student KS2 & KS1 Acceptable Use Policies

Online Safety Policy

Appendix 2

Pupil Acceptable Use Policies (KS2 / KS1)

Acceptable use of the school's ICT systems and internet: agreement for KS2 students and parents/carers

Name of student:

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

- Use them for a schoolwork or homework
- Use them only with a teacher being present, or with a teacher's permission
- Not access any inappropriate websites
- Not access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Never use chat rooms
- Only videoconference call with a teacher present
- Never open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use only kind and appropriate language when communicating online, including in emails
- Never share my password with others or log in to the school's network using someone else's details
- Never give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Never arrange to meet anyone offline without first telling my parent/carer, or without an adult to accompany me

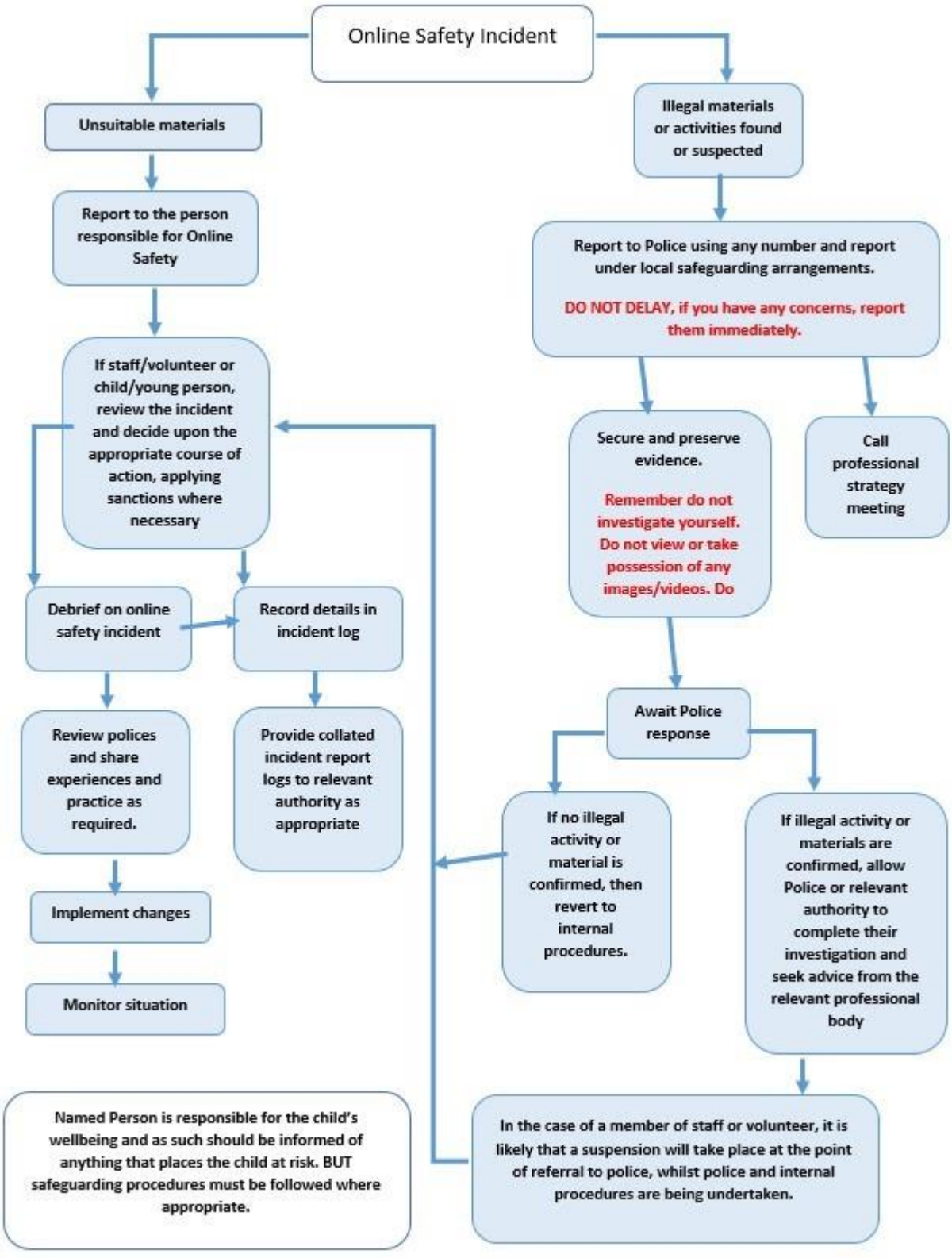
If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day, in any lesson times, clubs or other activities organised by the school, without a teacher's permission.
- I will hand my mobile phone into the office before school and collect it afterwards.
- 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.
- I will 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 will always use the school's ICT systems and internet responsibly.

Signed (student):	Date:

Acceptable use of the school's ICT systems and internet: agreement for EYFS/KS1 students and parents/carers	
Name of student:	
When using the internet in school, I will: • Only use it for school work. • Only use them when a teacher is there. • Only go on sites, which have been given by the teacher. • Not access social networking sites. • Not to use chat rooms • Never open anything that you are unsure about without asking a teacher. • Always use kind vocabulary when writing on the internet. • Never share any information with other people except your parents/carers • Never arrange to meet anyone offline without first telling my parent/carer, or without an adult to accompany me I will not bring a mobile phone or any other electronic device into school.	
Signed (student):	**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 students 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: Staff online safety incident flow-chart


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.