Online Safety Policy

This policy outlines Innovae2Educate Partnerships' aim to develop children's safe use of the internet, innovative technologies and digital communications as part of their blended learning curriculum.

This policy was approved as follows:			
Approver:	**Education Committee**	**Date:**	**12/03/25**
Owner:	Safeguarding	**Version:**	V1.0
LAC adoption date:	####	**Review frequency:**	2 yearly
Status:	Mandatory	**Next review date:**	February 2027

This policy applies to all - Innovate2Educate Partnership schools/ School Academy staff, pupils and parents.

Document History

Version	Version Date	Author	Summary of Changes
V1.0	January 2025	Liz Braithwaite	Full review of existing policy as well as policy reformatted using new template and Trust name change updated. Governance review required.

Contents

1. Purpose

To have robust processes in place to ensure the online safety of pupils, staff and volunteers both in school and remotely. To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology. To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Policy statement

This policy applies to all members of the school and Trust community (including staff, pupils, volunteers, parents/carers, visitors, and community users) who have access to and are users of school or Trust digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school/Trust. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the schools published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy is based on current legislation including:

The Education Act 1996 (as amended),The Education and Inspections Act 2006, The Equality Act 2010, The Education Act 2011, The Online Safety Act 2023, The Schools Act 2022, The Higher Education (Freedom of Speech) Act 2023.

And the Department for Education's latest guidance:

'Teaching Online Safety in Schools' (2019, updated June 2023), 'Preventing and Tackling Bullying' (2017, updated July 2023), 'Relationships, Sex and Health Education' (RSHE) (2019, updated September 2023), 'Searching, Screening and Confiscation: Advice for Schools' (2022, updated July 2023).

3. Definitions

A glossary of terms in included in the appendix of this document.

4. Responsibilities

General

Effective policies and procedures are in place and updated annually including a behaviour “code of conduct” for pupils, staff and volunteers with reference to online safety and should be read in

conjunction with "Guidance for Safer Working Practice for those who work with children in education settings". E-safety information is provided to the Local Authority (on behalf of the safeguarding partnerships) through the Safeguarding Annual Return.

Governance

The Local Academy Committee: The Local Academy Committee has a responsibility for reviewing the effectiveness of safeguarding procedures, including online safety, and escalating concerns to the Trust Board and CEO.

The Trust Board: The Trust Board is responsible for ensuring there are appropriate policies and procedures in place to safeguard and promote children's welfare. The Trust Board has a nominated designated board member for safeguarding and has oversight of the Trust's safeguarding arrangements and performance.

Local Academy Committee members and Trustees will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school/Trust IT systems and the internet

The headteacher

The headteacher is responsible for ensuring that:

- Staff understand this policy, and that it is being implemented consistently throughout the school.
- Staff receive suitable CPD to carry out their e-safety roles.
- There is a culture where staff and learners feel able to report incidents.
- There is a progressive e-safety curriculum in place.
- The DSL for e-safety monitors and evaluates incidents pertaining to e-safety across the whole school for pupils and staff.
- Correct Trust and local safeguarding partnership procedures are followed in the event of a serious e-safety allegation being made against a member of staff or pupil and informs the CEO about any serious e-safety issues.
- Reviews take place of the school's network infrastructure with a Senior Technician to ensure it is as safe and secure as possible and fit for purpose.
- Policies and procedures approved within this policy are implemented.
- The annual safeguarding audit reviews e-safety and actions are planned and accomplished to address any issues which may arise.

- The roles and responsibilities of the DSL for e-safety (as outlined below) are written in their job description and reviewed annually as part of their performance management.

The designated safeguarding lead for e-safety

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding leads (DDSL) are set out in our child protection and safeguarding policy.

The DSL for e-safety 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, IT technician team and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (MyConcern) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 5 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or Local Academy Committee members.
- Working with the Computing Lead and PSHE Lead in school to personalise the online safety curriculum in meeting the needs of the pupils.
- Ensuring that any online safety incidents are logged (MyConcern) and dealt with appropriately in line with this policy.

IT Technicians

IT technicians are responsible for:

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

- Conducting a full security check and monitoring the school's IT systems on at least a weekly basis.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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.

- They report any suspected misuse or problem to the DSL or DDSL for investigation and implement actions required of them.

- Ensuring that all digital communications with pupils/parents/carers should be open and transparent, on a professional level and only carried out using official school systems

- E-safety issues are embedded in all aspects of the curriculum and other activities

- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.

- Working with the DSL to ensure that any online safety incidents are logged (MyConcern) 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

Parents

Parents are expected to:

- Notify the school 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 IT systems and internet.

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

- What are the issues? - UK Safer Internet Centre

- Hot topics - Childnet International

- Parent factsheet - Childnet International

Visitors, volunteers and members of the community

Visitors, volunteers and members of the community who use the school's IT 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.

5. Educating pupils about online safety

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

1-2 lesson(s) every half term based upon the Digital Literacy and internet matters

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

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

In Key Stage 3 pupils will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 pupils will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- How to report a range of concerns.

By the end of secondary school, pupils will know:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- what to do and where to get support to report material or manage issues online;
- the impact of viewing harmful content;

- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;

- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail;

- how information and data is generated, collected, shared and used online;

- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;

- the safe use of social media and the internet will also be covered in other subjects where relevant;

- the school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The safe use of social media and the internet will also be covered in other subjects where relevant. E-Safety rules will be posted in any specific Computing Teaching and Learning areas and/or in all rooms where computers are used and discussed with pupils regularly.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information (Fake news) before accepting its accuracy.

Teachers will teach pupils to understand and follow the e-safety and acceptable use agreements.

Pupils will be taught to understand research skills, the need to avoid plagiarism, uphold copyright regulations, and critically evaluate AI-generated content while learning to use AI tools ethically as research assistants rather than substitutes for original thinking.

In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating parents about online safety

Parents may have only 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 the children's online behaviours. 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 therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL for e-safety.

Parents can report online safety concerns by:

1. Contacting the class teacher or form tutor
2. Emailing the designated safeguarding lead
3. Using the school's online reporting system
4. Attending regular online safety workshops and surgeries

7. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their pupils, and the issue will be addressed in assemblies.

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

All staff, local academy committee members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support pupils who may be affected. All schools have information on their websites to support the work undertaken on cyber bullying.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so. This will be in accordance with Keeping Children Safe in Education 2024 (Part 5: Child-on-child sexual violence and sexual harassment)

School Filtering and Monitoring

The school uses Wave 9 / Senso to filter and monitor online activity. These systems:

- Block access to inappropriate content
- Monitor search terms and website access
- Alert staff to potential safeguarding concerns
- Track attempted access to restricted content

Examining electronic devices

School staff have the specific power to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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

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

If inappropriate material is found on the device, it is up to the DSL or Headteacher to decide whether they should:

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

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

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

8. Acceptable use of the internet in school / data protection

All pupils, parents, staff, volunteers and governance members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

Use of live streaming within school will be monitored and only done in public view with a member of staff present. Privacy and safety settings are in place.

Pupils will be taught about online safe and unsafe behaviours to make sure that they are aware of what they are posting online. Pupils will know who to go to for help and how to report things that concern them.

We will monitor the websites visited by pupils, staff, volunteers, governance members and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices section.

Schools are subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the related policies section.

9. Pupils using mobile devices in school

Students are permitted to bring mobile phones to school for use during their journey to and from school only. During the school day:

All mobile phones must be switched off (never seen, never used, never heard) and stored securely in bags or lockers.

Phones must not be taken out or used at any time between arriving at and leaving school premises.

This includes before school, during lessons, break times, lunch times, and after-school activities or clubs.

Smart watches or other connected devices must be used in 'watch only' mode during school hours

If a student needs to contact home during the school day, they must do so through the school office. Similarly, if parents need to contact their child urgently, they should call the school office rather than their child's mobile phone.

Any phone seen or heard during school hours will be confiscated in line with the school behaviour policy. Confiscated phones will be stored securely in the school office and may be collected by students at the end of the school day. For repeated violations of the mobile phone policy, confiscated

phones will be stored securely in the school office and may only be collected by parents/carers at the end of the school day.

All use of mobile devices must comply with the school's acceptable use agreement (see appendix 1). The school accepts no responsibility for loss or damage to mobile phones brought onto school premises.

Any breach of the acceptable use agreement by a pupil will trigger disciplinary action in line with the school behaviour policy.

10. Staff using work devices outside school

Staff members must not install any unauthorised software on their work device and must not use the device in any way which would violate the school's / Trust terms of acceptable use, as set out in appendix 4.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. No USB devices containing data relating to the school/Trust must be used.

If staff have any concerns over the security of their device, they must seek advice from the IT technician team.

11. Staff using personal devices

Staff members must not use a personal device (this includes mobile devices such as mobile phones and tablets) to take or store images of pupils or staff. Contact details of pupils or parents should not be stored on personal devices. Personal mobile phones must not be used to contact pupils or parents. In exceptional circumstances, the headteacher may give permission for staff to make calls from personal devices, they should dial 141 first to hide their number for privacy purposes. During school outings, nominated staff will have access to a school mobile which can be used for emergency or contact purposes.

12. Technical Security Requirements

Technical Security and Data Protection

Staff must follow these technical security requirements:

Password Requirements:

- Use strong passwords that are at least 8 characters long
- Include a combination of upper and lower-case letters, numbers and special characters
- Change passwords regularly
- Never share passwords or reuse them across different systems

- Use two-factor authentication where available

Device Security:

- Ensure all devices have up-to-date antivirus software
- Keep operating systems and software updated
- Lock devices when not in use
- Use encryption for sensitive data
- Regular backup of important data

Cloud Storage:

- Use only approved cloud storage services (e.g., Office 365, TEAMS)
- Never store sensitive data on unauthorised cloud services
- Enable two-factor authentication for cloud service accounts
- Regularly review shared file permissions

13. How the school will respond to issues of misuse

Where a pupil 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, and will be proportionate.

Where a staff member misuses the school's IT 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. A flow chart for dealing with illegal incident (appendix 6) supports school in taking the correct action.

14. Incident Logging and Monitoring

All online safety incidents must be recorded using MyConcern, the school's safeguarding management software. All staff will log behaviour and safeguarding issues related to online safety using MyConcern. All online safety incidents must be recorded under the following categories:

- Social media concerns
- Cyberbullying
- Inappropriate searches
- Distributing obscene images

- Sexting
- Other online safety concerns

Child protection records are reviewed regularly by the Designated Safeguarding Leadership Team to check whether any actions are needed. This includes monitoring e-safety incidents such as patterns of complaints or concerns about any individuals and ensuring these are acted upon. Records of these reviews are kept in school (e.g., SLT/DSL meeting minutes, LAC meeting minutes).

The Central i2e Team will collate e-safety records and report this information to the CEO. Where a risk is identified, the CEO will add this to the school's risk register and support the school in addressing this. These risks will be reviewed regularly as part of the schools' risk assessment meetings.

All incidents must be recorded promptly and include sufficient detail to enable appropriate follow-up action while maintaining confidentiality where required.

DSLs will monitor online safety incidents through MyConcern's reporting features to identify patterns and inform preventive strategies.

A school's e-safety DDSL and/ or DSL will review online safety incidents termly as part of their regular safeguarding analysis.

15. Staff Training Requirements

Induction Training: All new staff must complete required documentation and training as part of their induction on or before their first day of employment:

- Basic online safety awareness
- Acceptable use policy review
- Safeguarding systems training
- Incident reporting procedures
- Device and system security

Annual Updates: Staff will receive annual safeguarding level 1 refresher training covering:

- New online threats and risks
- Policy and procedure updates
- System changes and security updates
- Best practice updates
- Incident response protocols

Specialised Training: DSLs and technical staff will receive additional training in:

- Data protection requirements
- Risk assessment

- Incident management

16. Related policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- GDPR policy
- Complaints procedure
- Staff handbook (incl. code of conduct)

17. Monitoring

The DSL, Deputy DSL's and/or class teachers will log behaviour and safeguarding issues related to online safety (MyConcern). E-safety incidents are logged using the following categories:

- Social media concern
- Cyberbullying
- Inappropriate searches
- Distributing Obscene images
- Sexting

Child protection records are reviewed regularly by the Designated Safeguarding Leadership Team to check whether any actions are needed. This includes monitoring e-safety incidents such as patterns of complaints or concerns about any individuals and ensuring these are acted upon. Records of these reviews are kept in school (e.g. SLT / DSL meeting minutes, AB meeting minutes).

18. Review

This policy will be reviewed every two years by the Central Team. At every review, any changes to the policy will be shared with the schools, Local Academy Committee and Trust Board as appropriate.

Appendix 1: Acceptable use agreement (KS2 pupils and parents / carers)

Acceptable use of the school's ICT systems and internet: agreement for KS2 pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will: Use them only 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	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (EYFS/KS1 pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for EYFS/KS1 pupils and parents/carers	
Name of pupil:	
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 (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (KS3/KS4/KS5 pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for KS3/KS4 pupils and parents/carers

Name of pupil:

As a student at an i2e school, I understand that access to the school's technology and internet is a privilege that comes with responsibilities. I agree to the following terms:

My Online Safety Commitment

I will keep myself safe by:

- Keeping all my passwords private and secure
- Never sharing personal information (like my address, phone number, or location) online
- Only communicating online with people I know in real life
- Never arranging to meet someone I've only met online without telling a responsible adult
- Being careful about what I share online, remembering that once something is posted, it can be difficult to remove
- Using strong passwords that are at least 8 characters long and changing them regularly
- Logging out of my accounts when I'm finished using them

My Digital Responsibility

When using school technology and the internet, I will:

- Only use my own login details and never share them with others
- Only access the internet for educational purposes during lesson time
- Only access websites that are appropriate for school use
- Reference any content I use from the internet in my work
- Report any inappropriate content I accidentally access
- Respect others' work and property online
- Follow the school's guidelines for online learning platforms and virtual classrooms

My Device Usage

If I bring a personal device (phone, tablet, smartwatch) to school:

- I will follow the school's rules about when and where I can use it – Never seen, Never used, Never heard
- I will keep it on silent/airplane mode during lessons unless given permission by a teacher
- I will not use it to access inappropriate content on the school premises

- I understand that the school can confiscate my device if I break these rules
- (KS5 Students ONLY) I will ensure my personal electronic device remains out of sight, turned off, and not in use when in the presence of younger students, only using it in designated work areas during my free periods.

My Online Behaviour

I will demonstrate good digital citizenship by:

- Being respectful in all my online communications
- Not engaging in cyberbullying or harmful online behaviour
- Not accessing, creating, or sharing inappropriate content
- Not downloading unauthorised software or files
- Not attempting to bypass the school's filtering systems
- Not using VPNs or proxy servers to access blocked content
- Thinking carefully about my digital footprint
- Supporting my peers if they face online issues

My Health and Wellbeing

I will look after my wellbeing by:

- Taking regular breaks from screens
- Maintaining good posture when using devices
- Being mindful of my screen time
- Balancing online and offline activities
- Speaking to a trusted adult if I'm worried about anything I see online

My Understanding

I understand that:

- The school monitors my internet use and digital communications
- Breaking these rules may result in disciplinary action
- The school may inform my parents/carers about any concerns
- The school may involve external agencies if necessary
- If I see something inappropriate, I should report it to a trusted adult immediately

Declaration

☐ I have read and understand this agreement

☐ I will follow these rules when using school technology ☐ I understand the consequences of breaking these rules	
Signed (pupil):	**Date:**
Parent/Carer Agreement As the parent/carer of this student: • I understand that my child has agreed to follow these rules • I will support the school in enforcing these guidelines • I will monitor my child's technology use at home • I will contact the school if I have any concerns about online safety • I understand that the school will contact me if there are concerns about my child's online behaviour	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement (staff, governors, volunteers and visitors)

Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the organisation's computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the organisations systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the organisations ethos, other appropriate policies, relevant national and local guidance and expectations, and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
- i2e Schools owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters and is changed regularly.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from your line manager or the IT network team.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site's (such as via email or on memory sticks or CDs) will be

encrypted by a method approved by the IT team. Any images or videos of pupils will only be used in line with organisational policy and will always take into account parental consent.

- I will never store or remove sensitive data from school systems, ensuring all confidential information remains secure within the school's protected network environment. Sensitive school data includes student and staff personal details, academic records, medical information, safeguarding documents, financial records, and any confidential information that identifies individuals within the school community. This protected information must always remain secure within school systems to maintain privacy and comply with data protection regulations.

- I will not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access the organisations email system on my mobile device (tablet or mobile phone), the device must be pin or password protected. I will protect the devices in my care from unapproved access or theft.

- Personal data kept on work devices must be kept to a minimum (examples that do not meet this include; Filling the hard drive with music files or photos).

- I will respect copyright and intellectual property rights.

- I have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I have read and understood the Loan Equipment policy that covers the use of any staff equipment that I may have been provided in order to carry out my work.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and line manager as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and my line manager.

- I will not attempt to bypass any filtering and/or security systems put in place by the organisation. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any organisation related documents or files, then I will report this to the IT network team as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.

- I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and the internet

will not undermine my professional role, interfere with my work duties and will be in accordance with the organisation's Acceptable Use Policy and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the organisation I work for into disrepute.
- I will promote online safety and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on staff member's work electronic devices.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……..

Print Name: …… Date: ……

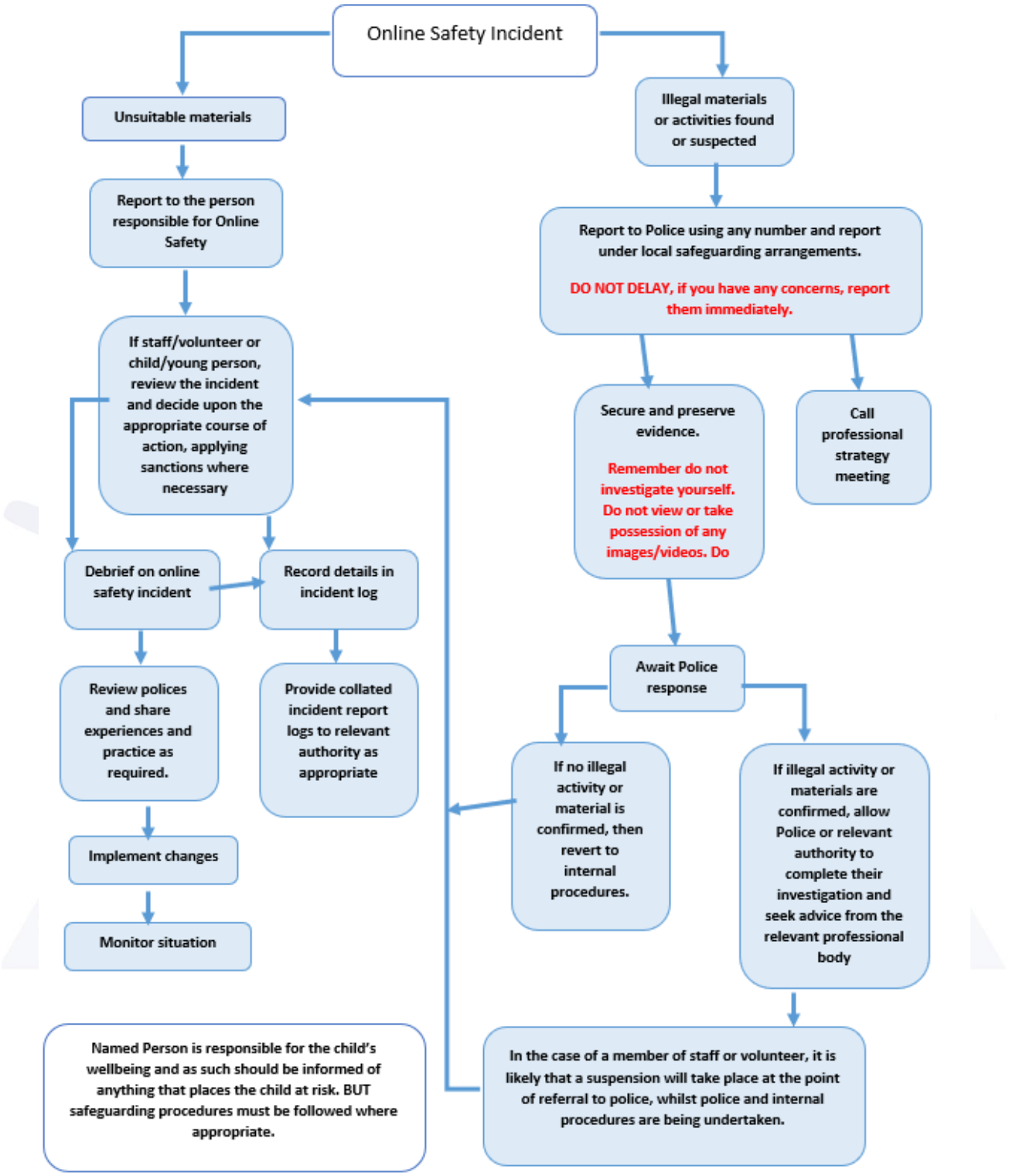
Appendix 5: Online training needs – self audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governance members and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you follow good password security practices by changing your school ICT system passwords at least twice a year, avoiding password reuse, and using unique passwords across different platforms?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 6: Flow chart for dealing with illegal incidents

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Appendix 6: Remote online learning etiquette for pupils

Remote Online Learning Etiquette for Pupils

Be respectful

While it is easier to say hurtful or disrespectful things without standing face-to-face with someone, it is important to remember that your classmates and teachers are real people who are affected by the words you say and write. It is essential to keep in mind the feelings and opinions of others, even if they differ from your own. **If you wouldn't say it to someone's face, don't say it online either.**

Be aware of strong language, all caps, and exclamation points

It is easy for written text to be misread and misunderstood. Have you ever sent a text message with good intentions, but your friend thought you were being rude? If so, then you've experienced this firsthand. Remember if you type in ALL CAPS it will look like you're screaming. By being alert to the language you use, you can stop potential confusions before sending messages. **Tip: Read everything out loud before you send it.**

Be careful with humour and sarcasm

Certainly, you shouldn't avoid being funny. We love to see your personality shine through in online classes. Many of our teachers are exceptionally funny too. But like mentioned above, make sure that it is clear you are being funny and not being rude, without your tone of voice your classmates may not know you are joking. Emoticons and smileys can be helpful when conveying humour or sarcasm so that it is read correctly. Just remember to keep the smiley faces away from schoolwork. 😉

Be forgiving

Remember that not everyone will know these rules before posting. Try to be understanding of others when they struggle with written communication. It is very different than simply talking to a person face-to-face. Respect and acknowledge that other classmates may have a different opinion to you and will post things differently than you, it doesn't mean either of you are right or wrong.

Try to stay on topic

Whenever you post a comment, thoughts, pictures or work remember to keep this about the topic or assignment you have been given. Reading through irrelevant posts takes time away from the learning you need to be doing. If you have a question, before posting check it hasn't been answered already further up the screen. Be brief, if you write lengthy posts people may not want to read it all. Tag in the person you want to see it in your reply so they get an alert and can be taken straight to your post instead of having to search for it.

Appendix 7: Online Safety Resources

For Schools:

- Thinkuknow - CEOP's educational resources
- Childnet International - Teaching resources
- UK Safer Internet Centre - Professional helpline
- Internet Matters - Parent resources
- NSPCC Online Safety - Research and guidance

For Parents:

- Parent Info (http://parentinfo.org) - Expert information
- Common Sense Media (https://www.commonsensemedia.org) - Reviews and advice
- Internet Matters (https://www.internetmatters.org) - Age-specific advice
- Net Aware (https://www.net-aware.org.uk) - Social media guides

For Students:

- BBC Own It (https://www.bbc.com/ownit) - Wellbeing resources
- Childline (https://www.childline.org.uk) - Support and advice
- Zipit App - Dealing with unwanted images
- Report Harmful Content - Reporting tools

Appendix 8: SCHOOL STAFF LOAN EQUIPMENT POLICY

SCHOOL STAFF LOAN EQUIPMENT POLICY

Purpose

This policy outlines the terms and conditions for school staff borrowing equipment owned by the school for work-related purposes.

Equipment Provision

The school may provide staff with equipment including but not limited to laptops, tablets, mobile phones, cameras, and other digital devices to enable them to fulfill their professional duties effectively.

Staff Responsibilities

1. **Care and Maintenance**
    - Staff must take reasonable care of all loaned equipment and maintain it in good working order
    - Any damage, loss, or theft must be reported to the IT network team/School Office immediately
    - Equipment should be kept in appropriate protective cases/covers when provided
2. **Acceptable Use**
    - Loaned equipment is primarily for work-related purposes
    - Limited personal use is permitted provided it does not:
        - Interfere with work responsibilities
        - Incur additional costs to the school
        - Compromise school data or systems
    - Equipment must not be used for any illegal, inappropriate, or commercial activities
3. **Data Security**
    - No sensitive school data should be stored on equipment outside secure school systems
    - Staff must ensure equipment is password protected at all times
    - Passwords must be changed regularly (at least every 6 months)
    - Staff must not allow unauthorised persons to use school equipment
4. **Return of Equipment**
    - All equipment remains the property of the school and must be returned:
        - Upon request
        - When employment ends
        - When going on extended leave
        - When damaged and in need of repair
    - All school data must be removed from the device upon return
5. **Costs and Liability**
    - Staff may be held financially responsible for equipment that is lost, stolen, or damaged due to negligence
    - The school will cover reasonable repair costs for normal wear and tear

Failure to comply with this policy may result in:

- Withdrawal of equipment
- Disciplinary action
- Financial liability for replacement/repair costs

By accepting school equipment, staff acknowledge they have read, understood, and agree to abide by this policy.

Staff Member Signature _____ School Representative_____

Date: Date: