Online Safety Policy

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

Version number	V2.1
Consultation groups	IT Leads
Approved by	Trust Board
Approval date	16.9.2020
Adopted by	Advisory Board
Adopted date	School to complete
Implementation date	September 2020
Policy/document owner	Liz Braithwaite
Status	Mandatory
Frequency of review	2 years
Next review date	September 2022
Applicable to	All staff

Document History

Version	Version Date	Author	Summary of Changes
V1.0	20/9/18	Nathan Thirlby Liz Braithwaite	Policy drafted
V1.1	29/9/18	Laurie Davis	Added appendix 1b AUP for EYFS and KS1.
V1.2	20/11/19	Liz Braithwaite	Added appendix templates for more specific acceptable use agreements
V1.3	7/09/2020	Liz Braithwaite	Review and amendments made due to impact of COVID-19 upon teaching and learning practices and introduction blended learning. Appendix 5 and 6 added. Section 6 – educating parents on safety enhanced. Section 9 – allow schools to determine if pupils can bring in mobile devices to school and what context. Reference to cluster boards removed.
V2.1	13/10/2020	Helen Stockill	Reference to data protection act updated to 2018 in appendix 3 & Safer working practice reference updated

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, 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.

Braunstone Community Primary 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.

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 the most recent "Guidance for Safer Working Practice for those who work with children in education settings".

An annual safeguarding and wellbeing audit including e-safety is completed by the head of safeguarding and pupil wellbeing and outcomes reported back to the Trust Board and Advisory Board through an annual action plan and risk assessment. Headteachers review the Safeguarding and Wellbeing action plan termly. E-safety information is also provided to the Local Authority (on behalf of the safeguarding partnerships) through the Safeguarding Annual Return.

Governance

The Advisory Board

The Advisory Board has a responsibility for reviewing the effectiveness of safeguarding procedures, including online safety, and escalating concerns to the Trust Board and the Head of Safeguarding and Pupil Wellbeing.

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 Chair of the Trust Board is the designated board member for safeguarding and has oversight of the Trust's safeguarding arrangements and performance.

Advisory Board 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 (appendix 2)

The headteacher / head of school

The headteacher/ head of school 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 (CPOMS).
- 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 children 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 Head of Safeguarding & Pupil Wellbeing, Director of IT and Trust Leader about any serious e-safety issues.
- Reviews take place of the school's infrastructure/network with the Director of IT or 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 with the school's Safeguarding and Head of Safeguarding & Pupil Wellbeing 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 deputies are set out in our child protection and safeguarding policy.

Sharon Rushin/ Lizzie Wright 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, IT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (CPOMS) 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 3 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 Advisory board.
- Working with the Computing Lead in school to personalise the online safety curriculum in meeting the needs of the pupils.
- Ensuring that any online safety incidents are logged (CPOMS) 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's behaviour policy.

The IT Technician

The IT technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's 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 a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Head of Safeguarding & Pupil Wellbeing

The Head of Safeguarding & Pupil Wellbeing is responsible for:

- Monitoring and supporting all schools so they meet compliance expectations and are developing online practice.

- Carrying out audits of safeguarding including e-safety arrangements as set out in this policy.
- Supporting schools with parental engagement around online safety.
- Keeping schools informed on developments and updates within e-safety through DSL network meetings.
- Facilitating the delivery of a high quality curriculum for e-safety, safeguarding and wellbeing in schools.

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 (Deputy DSL) 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (CPOMS) 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 (appendix 1)

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

- What are the issues? - UK Safer Internet Centre
- 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 (appendix 2).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
1 lesson every half term will be based upon the Project Evolve E-safety toolkit and curriculum. This toolkit provides progression throughout the school, rigorous coverage of the E-safety national curriculum objectives and provides lesson ideas, resources and key questions to support teachers with planning.

All children will also have 1 lesson per week on Computing where safe, respectful and responsible use of technology and the internet will be modelled and encouraged by staff in all of these lessons.

*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
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Particular attention will be paid to the safe and responsible use of Tapestry.com which is the platform KS1 children will use to access the school's blended learning opportunities
- identify what things count as personal information
- identify what is appropriate and inappropriate behaviour on the internet
- agree and follow sensible online safety rules, e.g. taking pictures, sharing information safely, storing passwords
- seek help from an adult when they see something that is unexpected or worrying
- demonstrate how to safely open and close applications and log on and log off from websites
-

*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
- to use Microsoft Teams and Century.com safely, respectfully and responsibly and will be given weekly opportunities to access these platforms in class as part of the school's blended learning opportunities
- reflect on their own digital footprint and behaviour online
- identify what is appropriate and inappropriate behaviour on the internet

- recognise the term cyberbullying and what it means
- agree and follow sensible online safety rules, e.g. taking pictures, sharing information, storing passwords.
- seek help from an adult when they see something that is unexpected or worrying
- demonstrate understanding of age-appropriate websites and adverts
-

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 the Computing Suite 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 and the need to avoid plagiarism and uphold copyright regulations

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
- Sharing information via Microsoft Teams and Tapestry.com

- Online learning competitions on Microsoft Teams, Times Table Rock Stars and Tapestry.com to promote E-safety and the use of technology in a safe environment. E.g. class rewards for the most minutes spent on Century.com engaging in learning activities or incentives for parents to engage with their children's online learning so they are more aware of what they are accessing online

- 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.

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

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. Class teachers will discuss cyber-bullying with their classes, 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, advisory board members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Braunstone Community Primary 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 children who may be affected. The school website shares the school's vision for E-safety as well as Social Media (Facebook, Twitter, Instagram, Snapchat) safe use checklists, a link to the CEOP (Child Exploitation and Online Protection Command) organisation and useful links to anti-cyber-bullying websites.

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 the Sexual Violence and Sexual Harassment between children in schools and colleges advice from the DFE.

Examining electronic devices
Braunstone Community Primary 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 (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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.

Children will be taught about online safe and unsafe behaviours to make sure that they are aware of what they are posting online. Children will know who to go to for help and how to report things that concern them (add DSL name for e-safety)

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 1 and 2.

Schools are subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the related policies section. The schools carries out a more detailed review of their data protection policies and procedures through the self-review tool – 360data.org.uk.

9. Pupils using mobile devices in school

Pupils may not bring mobile devices into school. If they do so they must be handed in at the office as soon as the child arrives and should be collected at the end of the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

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 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. 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.

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 use to contact pupils or parents. During school outings nominated staff will have access to a school mobile which can be used for emergency or contact purposes.

12. 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 5) supports school in taking the correct action.

13. 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. This will be through the schools own CPD programme.

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).

The DSL and Deputy DSL's 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.

Governance 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.

14. Related policies

This online safety policy is linked to our:

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

15. Monitoring

The DSL, Deputy DSL's and/or class teachers will log behaviour and safeguarding issues related to online safety (CPOMS). 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).

The Head of Safeguarding & Pupil Wellbeing will collate e-safety records and report this information to the Trust Leader. Where a risk is identified the Head of Safeguarding & Pupil Wellbeing alongside the IT Director 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' meeting.

16. Review

This policy will be reviewed every two years by the Head of Safeguarding & Pupil Wellbeing and the Director of IT. At every review, any changes to the policy will be shared with the schools, Advisory Board and Trust Board as appropriate through the meeting schedule in the Autumn term.

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

<table>
<tr><th colspan="2">Acceptable use of the school's ICT systems and internet: agreement for KS2 pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">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.
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 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.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

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

<table>
<tr><th colspan="2">Acceptable use of the school's ICT systems and internet: agreement for EYFS/KS1 pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 3: Acceptable use agreement (staff, governance members, 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.

1. 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**.**

2. Discovery 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.

3. 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 login as appropriate.

4. 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 6 or more characters and is changed regularly.

5. 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 Department.

6. 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 Department. Any images or videos of pupils will only be used in line with organisational policy and will always take into account parental consent.

7. 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.

8. 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).

9. I will respect copyright and intellectual property rights.

10. 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.

11. 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.

12. 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 your line manager.

13. 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 ICT Department as soon as possible.

14. 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.

15. 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 internet will not undermine my professional role, interfere with my work duties and will be in accordance with the organisations AUP and the Law.

16. 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.

17. 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.

18. 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 laptops.

19. 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: ……

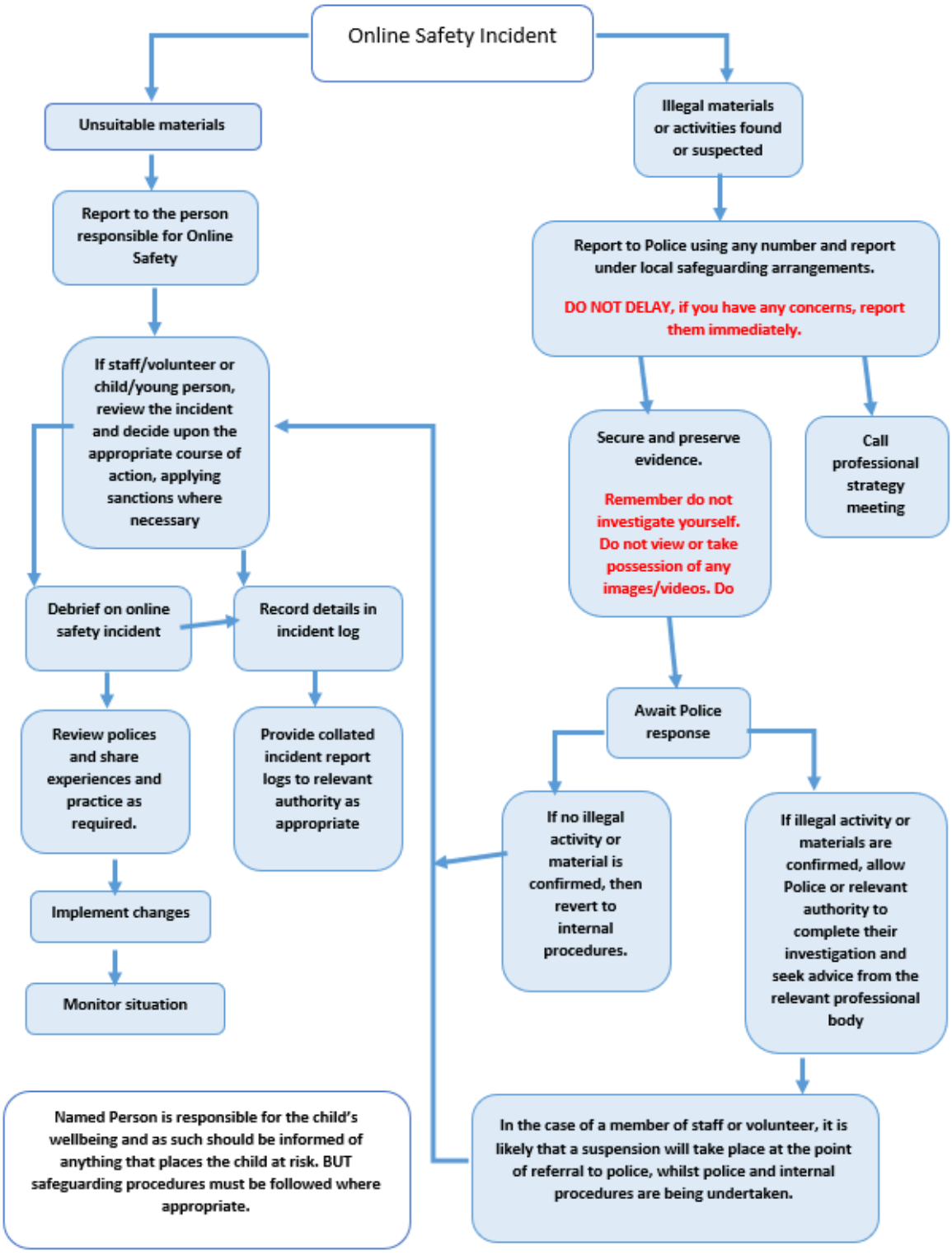
Appendix 4: Online training needs – self audit for staff

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 regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: 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.

Don't post or share (even privately) inappropriate material

Nothing is truly private online. Remember: If you wouldn't do or say something in real life, don't do it online either. If using a webcam remember to use it only in an appropriate room (not your bedroom) as we can all see what you are wearing and what is happening around you.

Yes, grammar and spelling matter

While texting, textspeak can b gr8 4 ur friends. In school (even online) however, keep it formal. Your written communication should reflect proper writing style. Save written shortcuts and 'text speak' for text messaging if you must but follow grammar rules for school. Check your spelling and punctuation before you post, make sure that what you are saying actually makes sense.