ST. AUGUSTINE OF CANTERBURY CATHOLIC PRIMARY SCHOOL

Online safety policy

Mission Statement

"I called you by your name, you are mine." Isaiah 43
The mission of our school is to support and further the teachings of Christ and His Church.
We welcome and embrace individuals of all abilities and cultural backgrounds.
We aim to enhance and celebrate their moral, physical, social and emotional development, so that they may reach their full potential in an atmosphere of stability, care and respect.
We believe that education is for all and in partnership with parents, carers, children and the wider Catholic community: we will strive and succeed in a wholly inclusive setting.

Date issued: February 2020

Date to be reviewed: February 2022

Written by: Mrs Claire Burns (Deputy DSL/Online safety lead)

Contents

1. Aims

2. Legislation and guidance

3. Roles and responsibilities

4. Educating pupils about online safety

5. Educating parents about online safety

6. Cyber-bullying

7. Acceptable use of the internet in school

8. Pupils using mobile devices in school

9. Staff using mobile devices in school

10. Staff using work devices outside school

11. Data Protection

12 Social Media - Protecting Professional Identity

13. How the school will respond to issues of misuse

14. Training

13. Monitoring arrangements

16. Links with other policies

17. Acknowledgements

18. Further Information and Support

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

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

Appendix 3: online safety training needs – self-audit for staff

Appendix 4: online safety incident report log and NSPCC incident report form

Appendix 5: Agreed User Actions

Appendix 6: Responding to incidents of misuse

1. Aims

St. Augustine of Canterbury Catholic Primary school aims to:

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying; searching, screening and confiscation, Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff and Relationships and sex education

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Karen McIntyre within her role as Safeguarding governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

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

3.3 The designated safeguarding lead

The school's designated safeguarding lead (DSL), Mrs Louise Prestidge and deputy designated safeguarding leads, Mrs Claire Burns and Mrs Angela Liggins take 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see appendix 4) 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 governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

At St. Augustine of Canterbury we have a managed ICT service provided by BCTEC. The school ensures that the managed service provider carries out online safety measures.

The ICT manager, BCTEC is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 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 (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (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: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Supply staff and visitors have temporary access onto the school systems through a separate log-on.

4. Educating pupils about online safety

4.1 National Curriculum

Children will be taught about online safety as part of the curriculum. From September 2020 all schools will have to teach Relationships education and health education in primary schools. This new requirement includes aspects about online safety.

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

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

By the end of primary school, pupils will know:

- That people sometimes behave differently 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

4.2 Wider curriculum opportunities

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum delivered through the Rising Stars Computing scheme of work as well as regular focussed online safety lessons, linked with our PSHE education provision.
- Key online safety messages are reinforced as during assemblies linked to national online safety awareness such as Safer Internet day.
- Children are taught in all lessons where applicable, to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children are helped to understand the need for Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school.
- All staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, children 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.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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.

4.3. Online-safety brigade

As part of our work for Safer Internet day, we appoint the children in Year 6 as members of the Online-Safety brigade. They work together with the class teachers to promote online safety in the other year groups. Together with the class teachers, the children plan lessons for the younger year groups to help them understand the importance of being safe on the internet.

4.4 SEND

Children with Special Educational Needs and Disability (SEND) are included within all areas of the curriculum, including the use of the internet for educational, creative, empowering and fun ways, just like their peers. However, they may be particularly vulnerable to online safety risks. For example:

- Children and young people with Autistic Spectrum Disorder may make literal interpretations of content, which will affect how they respond.
- Some children may not understand much of the terminology due to language delays or disorders.
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgements about what is safe information to share. This leads to confusion about why you should not trust others on the internet.

- There is also growing concern around cyberbullying. We need to remember that some children with SEN or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.

- In addition, some children may not appreciate how their own online behaviour may be seen by someone else as bullying.

These are challenging and complex issues which are addressed as part of any classroom differentiation or within individual children's learning plans, written in co-ordination with the Special Education Needs Co-ordinator (SENCO) Mrs Liggins, where relevant. Additional support for children with SEN can be found on Child's Net: http://www.childnet.com/resources/know-it-all-for-teachers-sen

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

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

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 other members of the DSL team.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or 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.

7. Acceptable use of the internet in school

All children, parents, staff, volunteers and governors 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.

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

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

8. Pupils using mobile devices in school

Children in Year 6, who walk to/from school may bring a personal mobile phone into school with permission from the class teacher. These are collected in the morning and stored securely in the school office. They are returned to the children at home time.

Children are not permitted to use these during lessons, on the playground before or after school, during clubs before or after school, or during any other activities organised by the school.

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

Any breach of the acceptable use agreement by a child may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Use of school mobile devices are permitted with the following conditions:

- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity on school owned devices. All unnecessary images or videos will be deleted immediately
- School owned devices may be used in lessons in accordance with teacher direction.

9. Staff using mobile devices in school

Staff are permitted to bring their personal mobile devices under the following conditions:

- Personal devices are brought into the school entirely at the risk of the staff member and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;
- Mobile phone devices should not be used in the presence of children. Mobile devices must be in silent mode and stored out of sight.
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school.
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances. Mobile phones should never be used in class during teaching sessions.
- Printing from personal devices will not be possible.

- Photographs and video images are not permitted to be taken with a personal device. Only school devices are permitted for such use in accordance with photography and video permissions.

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT managers, BCTEC.

Work devices must be used solely for work activities.

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.

- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media:
- The data must be encrypted and password protected.
- The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school / academy policy (below) once it has been transferred or its use is complete.

12. Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to children, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders

- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school disciplinary procedures

13. How the school will respond to issues of misuse

Where a child misuses the school's ICT 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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

See appendix 5 – Agreed User Actions, Dealing with Misuse and Sanctions – for more detail.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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.

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

Volunteers will receive appropriate training and updates, if applicable.

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

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log and NSPCC incident report form can be found in appendix 4.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. At every review, the policy will be shared with the governing board.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

17. Acknowledgements

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

https://www.nspcc.org.uk/globalassets/documents/information-service/esat-briefing-sample-e-safety-incident-report-form.pdf

https://www.thinkuknow.co.uk/parents/

http://www.childnet.com/parents-and-carers

http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/

18. Further Information and Support

Please see Internet Matters for definitions of different technologies:

https://www.internetmatters.org/advice/glossary/

The following is not exhaustive but should provide a useful starting point (KCSIE 2018, Appendix C):

- www.thinkuknow.co.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.childnet.com/cyberbullying-guidance
- www.pshe-association.org.uk
- http://educateagainsthate.com/
- www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
- https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis - external visitors and online safety

Appendix 1:

Staff, Governors, Volunteers and Visitors Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policy.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless authorised to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school / ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Appendix 2: acceptable use agreement

The Acceptable use agreements for EYFS/ KS1 can be found on our school website here:

http://www.staccp.org.uk/uploads/Policies/NEW/2017/acceptable%20use%20agreement%20policy%20EYFS-KS1.pdf

The Acceptable use agreement for KS2 can be found on our school website here:

http://www.staccp.org.uk/uploads/Policies/NEW/2017/acceptable%20use%20agreement%20policy%20KS2.pdf

The Acceptable use agreement for Parents/Carers can be found on our school website here:

http://www.staccp.org.uk/uploads/Policies/NEW/2017/acceptable%20use%20Parents-Carers.pdf

Appendix 3: online safety 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, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

NSPCC

Sample e-safety incident report form

Name of school:		
Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident? Child/young person ☐ Name of child..... Staff member/ volunteer ☐ Name of staff member/ volunteer..... Other ☐ please specify.....		
Description of incident (including IP addresses, relevant user names, devices and programmes used)		
Action taken: ☐ Incident reported to head teacher/senior manager ☐ Advice sought from Safeguarding and Social Care ☐ Referral made to Safeguarding and Social Care ☐ Incident reported to police ☐ Incident reported to Internet Watch Foundation ☐ Incident reported to IT ☐ Disciplinary action to be taken ☐ E-safety policy to be reviewed/amended ☐ Other (please specify)		
Outcome of investigation:		

Appendix 5: Agreed User Actions

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

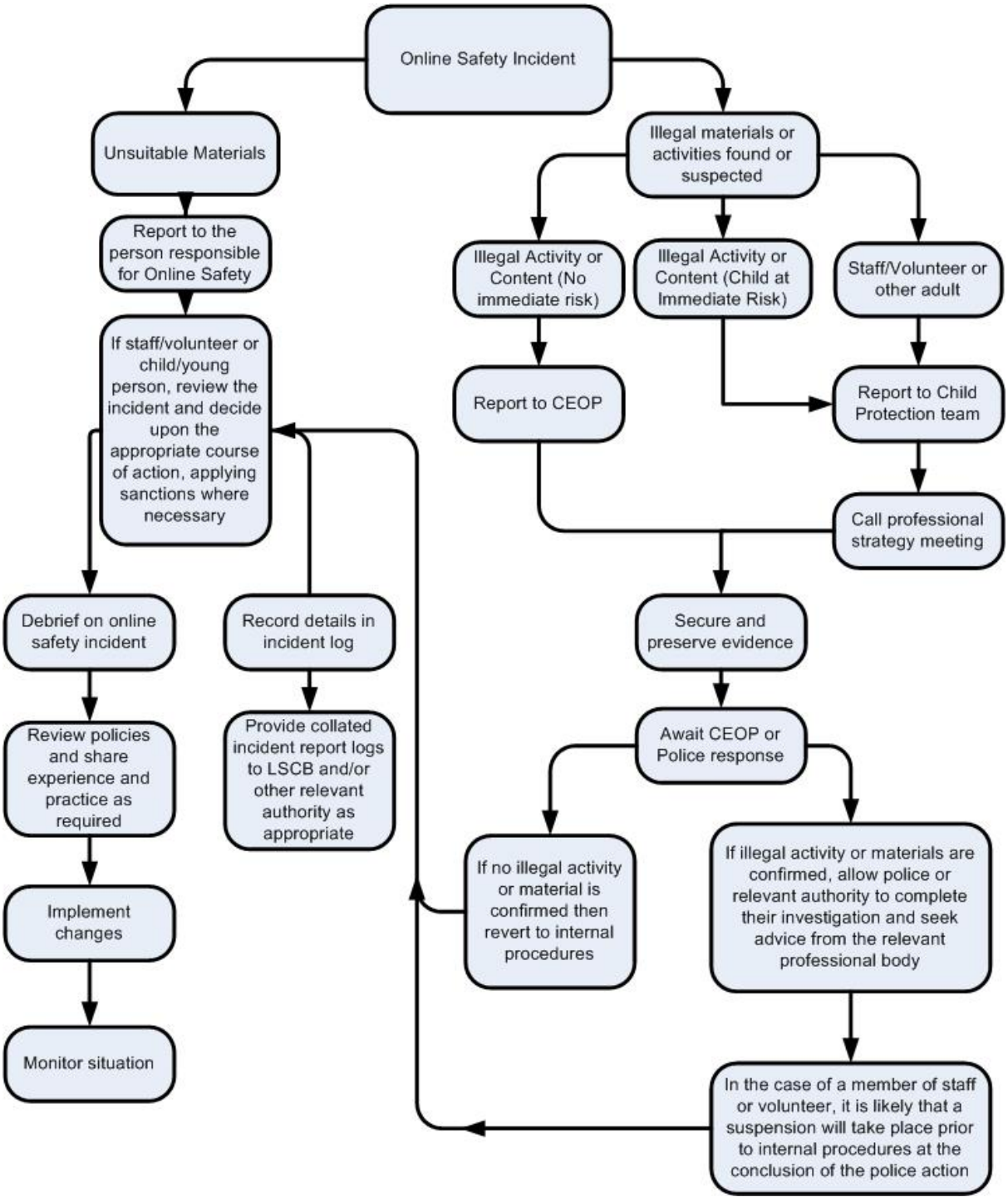
On-line gaming (educational)	X				
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube			X		

Appendix 6: Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "Agreed User Actions" above).

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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class	Refer to KS	Refer to	Refer to Police	Refer to	Inform	Removal of	Warning	Further
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	x							x	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x				x			
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x				x		x	
Unauthorised downloading or uploading of files	x	x						x	
Allowing others to access school network by sharing username and passwords	x							x	
Attempting to access or accessing the school network, using another pupil's account	x	x						x	
Attempting to access or accessing the school network, using the account of a member of staff		x	x			x			
Corrupting or destroying the data of other users		x	x			x		x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x	x	x	
Continued infringements of the above, following previous warnings or sanctions			x			x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x			x			
Using proxy sites or other means to subvert the school's filtering system			x		x				
Accidentally accessing offensive or pornographic material and failing to report the incident			x		x			x	
Deliberately accessing or trying to access offensive or pornographic material			x	x					x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x		x				

	Actions / Sanctions							
Staff Incidents	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	x					x		
Unauthorised downloading or uploading of files		x			x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			x	x		
Deliberate actions to breach data protection or network security rules		x	x			x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x			x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x					x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x				x		
Actions which could compromise the staff member's professional standing		x	x			x		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x				x		
Using proxy sites or other means to subvert the school's / academy's filtering system		x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x			x		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x				x
Breaching copyright or licensing regulations		x	x		x			
Continued infringements of the above, following previous warnings or sanctions		x	x					x