Online Safety Policy Curnow School

Date of Last Review: May 2024 Date of Next Review: May 2025

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online-safety policy is used in conjunction with other school policies (e.g. behaviour, PSHE anti-bullying and child protection policies).

It is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This policy supports this by identifying the risks and the steps we are taking to avoid them. "The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/) (DfE Keeping Children Safe in Education 2023)

1. Development and Monitoring

Role	Named Person
Computing Co-ordinator	Emily Birch
Designated Safeguarding Lead	Rob Armstrong
Senior Information Risk Officer	Rob Armstrong

This online-safety policy has been developed by the Computing Co-ordinator and the Designated Safeguarding Lead in conjunction with the School Leadership team. As part of this policy, records will be maintained (Cpoms) of Online-Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors, including CPOMs online tagging.
- Logs of reported incidents

2. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 cyber-bullying or other on-line e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy.

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

3. Roles and Responsibilities Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

Headteacher / Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Co-ordinator/Designated Safeguarding Lead.
- The Headteacher is responsible for the implementation and effectiveness of this policy. He is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Coordinator/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (SPT Disciplinary policy)
- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child / children, via any cloud-based website, Learning Platform or Gateway, have adequate information and guidance relating to the safe and appropriate use of this online facility
- The Headteacher is responsible for ensuring that Governors have adequate information and guidance about maintaining e-safety whilst carrying out their duty and that they comply with the policy.

Computing Co-ordinator + Designated Safeguarding Lead

The Computing Co-ordinator + Designated Safeguarding Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Reports to the School Leadership Team serious breaches of the E-Safety Policies
- Provides training and advice for staff
- Liaises with the Local Authority

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Are trained in and shares with staff and Governors an awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise from:
  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying
  - Sexting
  - Revenge pornography
  - Radicalisation (extreme views)
  - CSE

Teaching, Support Staff and Governors

Teaching, Support Staff and Governors are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the E–Safety policy, school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Computing Co-ordinator/ Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level
- Students / pupils understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy
- Students / pupils understand and follow E-Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our promoting positive behaviour and anti bullying policies.
- In lessons where internet use is planned, students / 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 (report to DNS/Cpoms).

Pupils

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc.
- Should understand that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local e-safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement
- Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

4. Education and Training Education – Pupils

Online-Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned e-safety programme should be provided as part of Computing/ PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students / pupils are taught the importance of keeping information such as their password safe and secure.
- Rules for the use of ICT systems / internet will be made available for pupils to read
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Students / pupils are taught how to keep safe though effective / good E-Safety practice as part of an integral 'Digital Literacy' element of the school Computing curriculum and within their ICT learning.
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Parents and Carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report, 2008 'Safer Children in a Digital World').

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

- Termly online safety newsletters, website updates
- Parents evenings
- Reference to external E-Safety websites
- High profile events such as Safer Internet Day
- Family learning opportunities

Education and Training – Staff and Governors

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required

5. Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, (DNS) in ways that ensure that the school meets the e-safety technical requirements for the Local Authority.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems

Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- The school maintains and supports the managed filtering service provided by DNS
- Any incidents or activities regarding filtering will be handled in accordance with DNS
- Remote management tools are used by the managed service provider to control workstations and view users activity
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- Guest access to the school network will be authorised by the School Office Team through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.
- The school infrastructure and individual workstations are protected by up to date antivirus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy.

6. Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission

- Written permission from parents or carers will be obtained before photographs of students/pupils together with their name are displayed on school displays, in newsletters and in their child's learning journeys / Evidence for Learning profiles.
- Written permission from parents or carers will be obtained before photographs of students/pupils together with their name displayed alongside are published in leaflets, posters, documents, training materials or used by the press.

  Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website or social media. Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school's Data Retention Policy.

In summary, personal data will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must be aware that a breach of the Data Protection Act may result in the school or an individual fine

Staff must also ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices or via any online Learning Platform or SMIS 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, USB 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 policy once it has been

8. Communications

When using communication technologies, the school considers the following as good practice:

The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the E-Safety Coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Students will be assigned individual school email addresses. These are to be used by learners / parents when accessing any Teams invites where learners will be accessing remote learning or where parents will be attending remote assemblies.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil or parent/carer. – may be occasions where contacting a parent has to happen, i.e. during remote learning, working from home, or in an emergency when an ambulance has been called – in which case, staff phone number must be withheld.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed.

- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device
- Parents have the opportunity to access a parent page on Facebook in a sensible, appropriate manner. Class DoJo will be used to share work and communicate with parents in a safe, appropriate manner.
- Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites

9. Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material

Other criminal conduct, activity or materials

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed.

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.

10. Monitoring and review

This policy will be reviewed annually, or earlier if necessary in line with national and/or local updates.

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.