



"Working together to Succeed"

Oakridge E-Safety Policy

Autumn 2024

E- SAFETY POLICY

E-SAFETY POLICY

Development and Review of this Policy

The implementation of this policy will be monitored by the Curriculum Committee. The monitoring of the policy will take place annually or more regularly in light of any significant new developments in the use of technologies or new threats to E-Safety of incidents that have taken place.

1. Aims of the Policy

This policy covers the **safe** and correct usage of all technical devices. It also covers data protection, safeguarding and sets out a clear code of conduct for everybody involved in the school.

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

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

2. Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

2.1 Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports. The ICT Governor will also be responsible for E-Safety and their role will include:

- Regular meetings with the E-Safety Co-ordinator.
- Regular monitoring of E-Safety incident logs.
- Reporting to relevant Governors / committees / meetings.

2.2 Head Teacher and Senior Leadership Team:

- The Head Teacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, through the day to day responsibility for E-Safety will be delegated to the E-Safety Coordinator.

- The Head Teacher and (at least) 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.
- The Head Teacher/ Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

2.3 E-Safety Coordinator:

- leads E-Safety
- 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
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with The BCC Technical Team
- receives reports of E-Safety incidents and ensures they are logged to inform future E-Safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant meetings.

2.4 Technical staff (The BCC Technical Team):

Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E-Safety technical requirements and any Local Authority guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- internet access is filtered for all users
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the data protection act and GDPR is followed.

2.5 Teaching and Support Staff:

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 Staff Acceptable User Policy
- they report any suspected misuse or problem to the Head Teacher/Senior Leadership Team/ E-Safety Coordinator for investigation
- all digital communications with pupils/parents/carers are 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

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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.
- they have viewed appropriate YouTube footage in advance including the suitability of adverts (these should be skipped after a few seconds). Staff must ensure their computer/laptop is logged off if they are not using it.

2.6 Child Protection Officer/Safeguarding Designated Person:

Should be trained in E-Safety issues and be aware of the potential for serious child protection/safeguarding issues to 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.

NB. It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

2.7 Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil's Acceptable User Policy
- need to understand the importance of reporting abuse, misuse, cyber-bullying or access to inappropriate materials and know how to do so
- will be expected to know how to use mobile devices and digital cameras safely. They should also know about cyber-bullying.

2.8 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. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.

3. Education

3.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression.

This will be provided in the following ways:

- A planned E-Safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the Pupil's Acceptable User Policy and encouraged to adopt safe and responsible use both within and outside school.
- 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, it is best practice that 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

3.2 Education – Parents/Carers

The school will take every opportunity to help parents understand these issues through parent's evenings, newsletters, school website and information about national/local E-Safety campaigns/literature. 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 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 including information sessions.
- Letters, newsletters, website.
- Parent's evenings.
- High profile events/campaigns e.g. Safer Internet Day.

3.3 Education & Training – Staff/Volunteers

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. This will be regularly updated and reinforced.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and the Staff Acceptable User Policy.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The E-Safety Coordinator will provide guidance to individuals as required.

3.4 Training – Governors

Governors should take part in E-Safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology / E-Safety/health and safety/child protection.

This may be offered in a number of ways:

- Participation in school training / information sessions for staff or parents.
- Understand this policy and be involved with the annual review.

3.5 Technical- equipment, filtering and monitoring (BCC Technical Team)

All ICT assets are recorded on an inventory. Assets that are damaged or surplus to requirements have data removed by the School IT Technician before being collected and destroyed by a reputable company.

The BCC Technical Team are 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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted (the school is also responsible for this).
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the **The BCC Technical Team** who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username.
- The 'administrator' passwords for the school ICT system, used by the School IT technician must also be available to the Head Teacher and E-Safety Co-ordinator and kept in a secure place.
- The E-Safety Co-ordinator and **The BCC Technical Team** are responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the

school systems and data. The school infrastructure and individual workstations are protected by up-to-date virus software.

- Agreed provision is in place for temporary access of 'guests' onto the generic 'supply' account (e.g. trainee teachers, supply teachers, visitors).
- An agreed policy forbids staff from downloading executable files and installing programmes on school devices.

4. Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the 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.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/ pupils are published on the school website.

5. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, which states that personal data must 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.

The school must ensure that:

- 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.
- Every effort will be made to ensure that data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.

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 secure password protected devices

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

- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff/pupils/parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website.

6. **Social Media - Protecting Professional Identity**

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the

course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Teaching staff have been allowed access to YouTube; Staff are responsible for ensuring they have viewed the footage in advance including the suitability of adverts (these should be skipped after a few seconds). Staff must ensure their computer/laptop is logged off if they are not using it.

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 limiting access to personal information:

- Training to include: acceptable use; social media risks; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to students/pupils, 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.

7. **Mobile Devices**

Staff

Staff must not use mobile phones in lessons, during teaching time, while on playground duty and during meetings. Mobile phones will be switched off or put on 'silent' or 'discreet' mode, except in urgent or exceptional situations.

Pupils

School does not allow children to bring mobile phones into school. However, where this is permitted, phones will be stored safely in the office.

8. **Unsuitable / inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution.

In the event of suspicion, it is important that the device is not shut down as evidence could be erased but that it is removed to secure site. All matters should be reported immediately to the Head/E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with 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.

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
- other criminal conduct, activity or materials.

Lockdown/Remote Learning

During periods of lockdown/ remote learning, it is essential that this document is re-read by staff and followed. Children will be using the internet more and possible with less supervision whilst parents work. E-Safety must be emphasised to pupils during this time through the class teacher and assemblies.