Ysgol Treganna E-Safety Policy

Introduction

The primary aims of our e-safety policy are to:

- Outline the key principles expected of all members of Ysgol Gymraeg Treganna's community regarding the use of ICT technologies.
- Safeguard and protect the children and staff of Ysgol Gymraeg Treganna.
- Support school staff working with children to work safely and responsibly with the internet and other communication technologies, and to monitor their own standards and practices.
  Set clear expectations regarding behaviour related to the responsible use of the internet for educational, personal, or recreational purposes.
  Ensure all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and, where appropriate, disciplinary or legal action will be taken against such behaviour.
- Minimize the risk of misleading or malicious allegations made against adults working with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content.
- Lifestyle websites that promote harmful behaviours.
- Content related to hate.
- Content validation: how to check the validity and accuracy of online content.

Contact

- Grooming (sexual exploitation, radicalization, etc.).
- Online bullying of all types.
- Social or commercial identity theft, including passwords.

Behavior

- Aggressive behaviours (bullying).
- Privacy issues, including the disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (time spent online, gambling, body image).
- Sexting.
- Copyright (lack of care or consideration for intellectual property and ownership).

Scope
This policy applies to the entire school community, including the Senior Leadership Team of Ysgol Gymraeg Treganna, the school's governing board, all staff employed directly or indirectly by the school, and all pupils.

The Senior Leadership Team and the school's Governing Board will ensure that any relevant or new legislation that may affect the provision for e-Safety in the school is reflected in this policy.

The Education and Inspections Act 2006 empowers headteachers, to a reasonable extent, to regulate the behaviour of students or pupils when they are off the school premises and empowers staff members to enforce disciplinary penalties for inappropriate behaviour.

This applies to incidents of cyberbullying or e-safety incidents covered by this policy that may occur outside of school but are linked to school membership.

The school will clearly outline its control over incidents within this policy, related behaviours, and anti-bullying policies and, where known, will inform parents and carers of incidents of inappropriate e-safety behaviour outside of school.

Review/Ownership
The online safety policy is referenced within other school policies (e.g., Child Protection and Safeguarding policy, Anti-Bullying policy).

The school has appointed an e-Safety coordinator who will be responsible for the ownership, review, and updating of documents.

The e-Safety policy was written by the school's e-Safety coordinator and is current and appropriate for its intended audience and purpose.

The online safety policy will be reviewed annually or whenever significant changes are made to the technologies used in the school.

There is broad ownership of the policy, which has been agreed upon by the SLT and approved by the Governors. All changes to the school's online safety policy will be shared with all staff and pupils.

Communication Policy

We believe that e-Safety is the responsibility of the entire school community, and everyone has a role to play in ensuring that all members of the community can benefit from the opportunities technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community will contribute:

Staff/pupils/community members will be informed of the policy in the following ways:

- The policy will be posted on the school website/staff room/classrooms.
- The policy will be included as part of the school induction pack for new staff.
- Regular updates and training on online safety will be provided to all staff.
- Acceptable use agreements will be discussed with staff and pupils at the start of each academic year.

- Acceptable use agreements will be issued to the entire school community upon joining the school.

Roles and Responsibilities

Senior Leadership Team (SLT):

- The headteacher is ultimately responsible for the provision of e-Safety for all members of the school community, although day-to-day responsibility for e-Safety is delegated to the e-Safety coordinator.
- The headteacher and the SLT are responsible for ensuring that the e-Safety coordinator and relevant staff receive appropriate training to fulfill their e-Safety roles and train colleagues as necessary.
- The headteacher and SLT will ensure arrangements are in place to monitor and support those in the school who carry out e-Safety monitoring roles. This provision offers a safety net and supports colleagues undertaking critical monitoring responsibilities.
- The SLT will receive monitoring reports from the e-Safety coordinator.
- The headteacher and SLT should ensure they are aware of the procedures to follow in the event of a serious e-Safety incident.
- The headteacher and SLT will receive an updated report from the incident management team.

Responsibilities of the e-Safety Coordinator:

- Promote awareness and commitment to e-Safety across the school and act as the first point of contact on all e-Safety matters.
- Be responsible for the day-to-day management of e-Safety in the school and play a leading role in establishing and reviewing the school's e-Safety policies and procedures.
- Lead the school's e-Safety pupil group or committee.
- Maintain regular contact with other e-Safety committees, e.g., Local Authority and Local Safeguarding Department.
- Communicate regularly with the school's technical staff (iTeach).
- Liaise regularly with the designated e-Safety governor.
- Liaise regularly with the SLT.
- Create and maintain e-Safety policies and procedures.
- Develop an understanding of current e-Safety issues, appropriate guidance, and legislation.
- Ensure all staff receive appropriate training in e-Safety issues.
- Ensure e-Safety education is embedded across the curriculum.
- Promote e-Safety to parents and carers.
- Monitor and report e-Safety issues to the SLT as appropriate.
- Ensure all staff are aware of the procedures to follow in the event of an e-Safety incident.
- Ensure the e-Safety incident log is updated.
- Ensure the school's e-Safety policy is up-to-date and relevant.
- Ensure the school's e-Safety policy is reviewed at pre-arranged times.
- Ensure the school's Acceptable Use Policies are appropriate for their intended audience.
- Promote the safe use of the internet and any technologies used in the school to all members of the school community.

Responsibilities of Teachers and Support Staff:

- Read, understand, and help promote the school's e-Safety policies and guidance.
- Report any suspected misuse or problem to the e-Safety coordinator.
- Develop and maintain an awareness of current e-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Ensure that any digital communication with pupils is conducted professionally and exclusively through school systems, never through personal mechanisms, such as email, text messages, or mobile phones.
- Embed e-Safety messages into learning activities across all areas of the curriculum.

Responsibilities of Staff and Support Staff

- Supervise and guide pupils carefully when participating in learning activities involving technology.
- Ensure pupils are fully aware of research skills and fully understand legal issues related to electronic content, such as copyright laws.
- Be aware of e-Safety issues related to the use of mobile phones, cameras, and mobile devices.
- Understand and be aware of the incident reporting mechanisms that exist in the school.
- Maintain a professional level of behaviour at all times when using technology for personal purposes.

Responsibilities of Technical Staff (iTeach):

- Read, understand, contribute to, and help promote the school's e-Safety policies and guidelines.
- Read, understand, and adhere to the school staff's Acceptable Use Policy.
- Report any e-Safety issues to the e-Safety coordinator.
- Develop and maintain an awareness of current e-Safety issues, legislation, and guidance relevant to their work.
- Always maintain a professional level of behaviour in personal use of technology.
- Support the school in providing a secure technical infrastructure to support teaching and learning.
- Ensure access to the school network is restricted and authorized only through secure mechanisms.
- Ensure there are provisions for detecting misuse and malicious attacks.
- Take responsibility for the safety of the school's ICT system.
- Liaise with the local authority or trust and other appropriate individuals and organizations on technical matters.
- Document all technical procedures and review them periodically to ensure accuracy.
- Appropriately restrict all administrator-level accounts.
- Ensure access controls are in place to protect personal and sensitive information stored on school-owned devices.
- Ensure appropriate physical access controls are in place to manage access to information systems and telecommunication equipment in the school.
- Ensure appropriate backup procedures are in place so that critical information and systems can be restored in the event of a disaster.

- Ensure controls and procedures exist so that access to software assets owned by the school is restricted.
- Be part of the incident management team that meets every term to review e-Safety incidents that have occurred in the school.

Responsibilities of Pupils:

- Help and support the school in creating e-Safety policies and practices and adhere to any policies and practices the school creates.
- Be aware of and understand the school's policies on the use of mobile phones, digital cameras, and mobile devices.
- Be aware of and understand the school's policies on cyberbullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely at school and at home.
- Be fully aware of research skills and legal issues related to electronic content, such as copyright laws.
- Take responsibility for ensuring safe and responsible use of technology by themselves and their peers at school and at home, including assessing the risks posed by personal technology owned by the school and used outside the school.
- Ensure they respect the feelings, rights, values, and intellectual property of others when using technology at school and at home.
- Understand what steps to take if they feel anxious, uncomfortable, vulnerable, or at risk while using technology at school or at home, or if they are aware that this is affecting someone else.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials and be fully aware of the school's incident reporting arrangements.
- Discuss e-Safety issues with family and friends openly and honestly.

Responsibilities of Parents and Carers:

- Help and support the school in promoting e-Safety.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use at school and at home.
- Take responsibility for their own awareness and understanding of the opportunities and risks posed by new and emerging technologies.
- Discuss e-Safety concerns with their children, show interest in how they use technology, and encourage safe and responsible behaviour when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult the school if they have any concerns about their children's use of technology.
- Agree to sign a home-school agreement to support the school's approach to online safety and refrain from uploading or sharing any images, videos, sounds, or texts that may cause distress or offend any member of the school community.
- Support the school's stance on the use of ICT systems and equipment.

If a parent adds a photo of their child on social media, we recommend that school logos are not visible to protect their child.

- Parents and carers are asked to read and sign acceptable use agreements on behalf of their

children upon admission to the school.
● Parents and carers are required to provide written consent for the use of any images of their children in various circumstances.

Responsibilities of the Governing Body

- Read, understand, contribute to, and help promote the school's e-Safety policies and guidelines.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an understanding of how the school's ICT infrastructure provides safe internet access.
- Develop an understanding of how the school encourages pupils to adopt safe and responsible behaviours when using technology both within and outside the school.
  Support e-Safety efforts by promoting and ensuring the safe and responsible use of technology within and outside the school, including encouraging parents to participate in e-Safety activities.
- Ensure appropriate funding and resources are available to the school to implement its e-Safety strategy.

Responsibilities of the Child Protection Officer/Safeguarding Officer

- Understand issues related to sharing personal or sensitive information.
- Understand the risks associated with accessing inappropriate online contact with adults and strangers.
  Be aware of potential or actual incidents involving the grooming of young children.
  Be aware of cyberbullying and the use of social media for this purpose.

Responsibilities of External Groups

- The school will liaise with local organizations to establish a common approach to e-Safety and the safe use of technologies.
  The school will be sensitive to and show empathy for issues related to the internet that pupils outside the school experience, e.g., social networking sites, and provide appropriate advice where needed.
- The school will provide an Acceptable Use Policy for any guests needing to use the school's computer systems or internet on school premises.
  The school will ensure appropriate levels of supervision are in place when external organizations use the internet and ICT equipment on school premises.

Management of Digital Content Systems and Communication

- Written consent will be obtained from parents or carers for the following scenarios before publishing photos of pupils. This will be done upon their admission to the school:
  - On the school website.
  - On the school's social media accounts (e.g., Instagram).
  - On the school's learning platforms (e.g., Seesaw for Nursery/Reception and Google Classroom/Teams for Key Stage 2).
  - On the school app (Group Ed).
  - In the school prospectus and other printed promotional materials (e.g., newspapers).
  - In display materials that may be used off-site.
  - Recorded or broadcasted via video or webcam in an educational conference.

Parents and carers can withdraw consent in writing at any time.

- Pupils will be reminded of safe and responsible behaviours when creating, using, and storing digital images, videos, and audio.
- Pupils will be reminded of the risks of inappropriate use of digital images, videos, and audio in their online activities at school and at home.
- School equipment will only be used for creating digital images, videos, and audio. In exceptional circumstances, personal equipment may be used with the headteacher's permission, provided that any media is transferred to school devices only and deleted from personal devices. Specifically:
  - No digital images, videos, or audio will be taken without the consent of participants.
  - Images and videos will reflect appropriate activities, and participants will wear appropriate attire.
  - Full names of participants will not be used either within the resource, in the file name, or in related online text.
  - Such resources will not be published online without the consent of the relevant staff and pupils involved.
  - If pupils participate, parental consent will also be requested before resources are published online.
- When searching for images, video clips, or audio, copyright rules and ownership recognition will be taught to pupils.

Storage of Images

- Any images, videos, or audio clips of pupils must be stored on the school network and must never be transferred to personal devices.
- The school will retain images of pupils who have left for two years after their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media to store any images, videos, or audio clips of pupils.

Password Policy

Pupils in the Foundation Phase and Key Stage 2 have login passwords for the school's ICT equipment, Hwb, and Teams. The school makes it clear that staff and pupils must always keep their passwords

private and must not share them with others. If a password is compromised, the headteacher or coordinator must be informed immediately.

- All staff have their own unique usernames and private passwords to access school systems. Staff are responsible for not disclosing their passwords. Passwords should not be written down. They should only be disclosed to authorized ICT support staff if necessary and to no one else. Any disclosed personal passwords must be changed as soon as possible. Personal passwords must always be entered manually when logging in. Do not include passwords in any automatic login procedures. The school keeps a record of all user access and their activities when using the system.
- Staff are required to use strong passwords. Passwords should be at least eight characters long, difficult to guess, and include numbers, letters, and special characters. The more random the password, the more secure it is. Users should create different passwords for different accounts and applications.
- Users should change their passwords whenever there are signs that the system or password has been compromised. Staff are required to change their passwords twice a year.
  Staff using critical systems are required to use two-factor authentication.

Emerging Technologies All new technologies will be tested and reviewed for any potential security vulnerabilities.

Appropriate countermeasures will be adopted in the school to ensure that any risks are managed to an acceptable level. Before any new technologies are used in the school, staff and pupils will receive appropriate training.
Using computer systems without permission or for improper purposes may constitute an offense under the **Computer Misuse Act 1990**, and details of breaches will be reported to the relevant authorities. Methods for identifying, assessing, and mitigating risks will be reviewed regularly.

Internet Access Filtering

The school uses a filtered internet service. The filtering system is provided by Cardiff Council using Smooth wall and includes filtering appropriate to the age and maturity of the pupils.

- If users discover a website containing inappropriate content, they should report it to a staff member, who will inform the e-Safeguarding Coordinator. All incidents will be recorded in the e-Safeguarding log.
- If users discover a website containing potentially illegal content, it must be reported immediately to the e-Safeguarding Coordinator. The school will report such incidents to the filtering provider—Cardiff Council.
- Pupils are taught to assess content as their internet usage skills develop. They will use age-appropriate tools to research internet content. Evaluating online content is part of teaching and learning in all subjects and will be considered a school-wide requirement across the curriculum.

Internet Access Authorization

- All staff and pupils will receive appropriate awareness training. Parents will be informed that pupils will access the web under supervision appropriate to their age and ability.
- When considering internet access for vulnerable members of the school community (e.g., children in care), the school will make decisions based on prior information.
- Responsible internet access for Foundation Phase pupils will be directly supervised by a responsible adult. Key Stage 2 pupils will be closely supervised and monitored while using the internet.
- Pupils will frequently be reminded of internet safety and safe use practices.

Email

- The school provides staff with an email account for professional use, and staff should be aware that any use of the school's email system will be monitored and checked.
- Anonymous or group email addresses will be used where appropriate, for example.
- The school will contact the police if staff or pupils receive emails considered particularly offensive or unlawful.
- The school will ensure email accounts are maintained and updated.
- Staff should not use personal email accounts during school hours or for professional purposes, particularly for exchanging any school-related information or documents.
- To ensure user safety, all emails are filtered and logged. A complete audit trail can be provided if necessary.
- Staff will use official school-provided email accounts for communication with pupils, parents, and carers. Under no circumstances should staff communicate with pupils, parents, or conduct any school business using personal email addresses.

Using Email

- Pupils may only use school-approved accounts on the school's system and only under the direct supervision of teachers for educational purposes.
- When using email, pupils and staff will be reminded to send polite and responsible messages.
- Pupils must not disclose personal details about themselves or others in emails.
- Communication between staff and pupils or members of the wider school community must be professional and related to school matters only.
- Staff email accounts should be checked regularly for new correspondence.
- Pupils and staff will be informed of the dangers of opening emails from unknown senders or sources, as well as the risks of opening attachments.
- Pupils and staff must never open attachments from untrustworthy sources.
- Any inappropriate use of the school's email system or receipt of inappropriate messages from another user should be reported to a staff member immediately.
- Pupils must immediately inform a teacher or trusted adult if they receive any email that makes them feel uncomfortable or concerned.

School Website

The headteacher has overall responsibility for ensuring the website's content is accurate and that its presentation is of high quality. Most of the material is the school's own work; where others' work is published or linked, sources are credited, and the author's identity or status is clearly indicated. No full names are associated with photographs published on the website. Pupils' names are not used when saving images as file names or tags for the school website.

Using Blogs, Wikis, Podcasts, Social Networks, and Other Online Publishing Platforms

Blogging, podcasting, and other forms of online publishing by pupils will take place at school and may be published on the school website. Pupils are not permitted to post or create content on websites unless the site has been approved by a teacher. Pupils will not use their real names when creating resources accessible to the public. They are encouraged to create appropriate pseudonyms. Personal publishing through websites appropriate for their age and educational purposes is taught. Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites, and other online publishing outside school.

Social Networking

Staff, Volunteers, and Contractors

- Staff are instructed to keep professional and private communicabon separate at all bmes.
- Teachers are advised not to maintain personal social network spaces for pupils or use their private spaces for interacbons with students. Instead, they should use the school's approved systems for such communicabons, following the school's communicabon policy.

In their private use of social media, school staff should ensure:

- No references to students/pupils, parents/carers, or school staff are made on social media.
- Staff do not become online friends with any student/pupil.
- They do not engage in online discussions about personal macers involving members of the school community.
- Personal opinions are not acributed to the school or the local authority, nor should personal opinions compromise their professional role or bring the school into disrepute.
- Security sedngs on personal social media profiles are checked regularly to minimize the risk of personal informabon loss.

Pupils:

- Pupils are taught about social networking, acceptable behaviours, and how to idenbfy misuse, threats, or abuse through our online safety curriculum.
- Pupils are required to sign and adhere to our age-appropriate Acceptable Use Agreement.

Parents:

- Parents are reminded of social networking risks and protocols through our Acceptable Use Agreement and addibonal communicabons when necessary.
- Parents are reminded to seek permission before uploading photos, videos, or any other informabon about others.

Mobile Phone Use in School

Staff Use of Personal Devices

- Mobile phones and personal devices must not be used during lessons or formal school bme.
- They should always be switched off or set to silent.
  The responsibility for mobile phones and personal devices brought to school lies with their owner. The school accepts no responsibility for the loss, thef, or damage of mobile phones or personal devices.
- Mobile phone Bluetooth funcbonality must be turned off at all bmes and should not be used to send images or files to other mobile phones.
  No images or videos may be taken on personal mobile phones or devices unless prior permission is obtained from the headteacher in excepbonal circumstances. Any such media must be uploaded to the school server and immediately deleted from the personal device.

Pupil Use of Personal Devices

- Pupils should not bring mobile phones or personal devices to school. The school accepts no responsibility for the loss, thef, or damage of pupils' mobile phones or personal devices.
- If a parent/carer chooses to give a pupil a mobile phone to use while walking to/from school alone, these will be kept in the office for the durabon of the school day. Upon entering the school, every pupil must hand their device to a member of staff, and these devices can be collected at the end of the school day.
- Pupils bringing a mobile phone or smart watch to school must sign an agreement alongside their parents acknowledging they understand the rules for using mobile/camera technology in school (Appendix 1).
- Breaches of these rules may lead to further disciplinary acbon.

Pupils will be instructed on the safe and appropriate use of mobile phones and personal devices and will be made aware of the rules and consequences. If a pupil breaches school rules, the phone or device will be confiscated and stored securely. Confiscated phones or devices will be handed over to parents or carers.

Parents are advised not to contact their child via their mobile phone during school hours but to contact the school office instead.

Role of Pupils

All pupils should be clear about the school's policy on mobile phone use and be reminded of it regularly. Pupils should be educated about the risks associated with using mobile phones, both in school and more broadly, including how to stay safe while walking home and using their phones.

Pupils should also be taught the benefits of having a mobile phone-free environment and be encouraged to see such an environment as desirable and valuable. This will help foster intrinsic motivation to support the school culture.

Role of Parents

Parents play a vital role in supporting the school's policy on banning the use of mobile phones in school and should be encouraged to reinforce and discuss the policy at home as appropriate, including the risks associated with mobile phone use and the benefits of a mobile-free environment.

If parents need to contact their child during the school day, they should be directed to the school office, where staff should be aware of the school's policy on relaying messages and facilitating contact.

Loss, Theft, or Damage

Pupils who bring phones to school must ensure they are properly labeled and stored securely in the office throughout the school day. Pupils must ensure their phones are switched off.

Staff must also secure their personal phones, as well as any work phones provided to them.

The school does not accept responsibility for the loss, theft, or damage of mobile phones on school premises or transport, during school visits or trips, or while pupils travel to and from school.

Parents and pupils will sign a home-school agreement acknowledging that the school accepts no responsibility for mobile phones under these circumstances (**Appendix 1**).

Lost phones should be returned to the school office. The school will then attempt to contact the owner.

Use of Laptops/iPads

The use of laptops and iPads by all staff is governed by an Acceptable Use Agreement signed by relevant staff. Laptops and iPads left in school overnight must be locked away securely. iPads must not be connected to individual iTunes accounts, and requests for apps must be submitted in writing to the ICT coordinator.

If staff are absent for an extended period (over two weeks), laptops and iPads must be returned to the school.

Teaching and Learning

We believe that the best way to develop safe and responsible online behaviors, not only for pupils but for everyone in our school community, is through effective education. We recognize that the internet and other technologies are embedded in the lives of our pupils, both at school and at home, and we believe it is our duty to help prepare our pupils to safely benefit from the opportunities provided by the internet.

- We will provide a series of specific e-Safeguarding lessons in every year group as part of the ICT curriculum and other lessons to achieve the following objecbves:

Nursery/Recepbon:

- Use ICT hardware to interact with age-appropriate sofware.

Years 1 and 2:

- Use technology safely and respeciully, keeping personal informabon private, and idenbfy where to seek help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2:

- Use search technologies effectively, learn how results are selected and ranked, and evaluate digital content critically.
- Use technology safely, respectfully, and responsibly; understand acceptable/unacceptable behaviour; and identify a range of ways to report concerns about content and contact.
- Participate in the annual **Safer Internet Day.**
  We will discuss, remind, or raise relevant e-Safeguarding messages with pupils as a matter of routine whenever appropriate opportunities arise during lessons, including:
  - The need to protect personal informabon.
  - Considering the consequences their acbons may have on others.
  - The importance of verifying the accuracy and validity of the informabon they use.
  - The importance of respecbng and acknowledging the ownership of digital materials.
- Any use of the internet will be carefully planned to ensure it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of online tools appropriate to their age safely and effectively.
  Staff will model safe and responsible behaviour when using technology during lessons.
  Pupils will learn how to search for information and evaluate website content for accuracy when using it in any curriculum area.
  When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored, and pupils will be reminded of what to do if they encounter unsuitable content.
- All pupils will be taught age-appropriate lessons on copyright in relation to online resources and will learn to understand ownership and the importance of respecting and acknowledging copyright for materials found online.
- Pupils will be taught about the impact of cyberbullying and will know how to seek help if affected by any form of online bullying.

- Pupils will know where to seek advice or help if they experience problems using the internet and related technologies (e.g., a parent or carer, teacher, or trusted staff member, or organizations such as **Childline**).

Remote Learning

If an isolation bubble needs to be established or the school needs to close, remote learning will provide the following:

- A variety of input/live lessons delivered by teachers and supported by Teaching Assistants via Google Meet. These sessions will be recorded.
- Tasks set on Seesaw, Teams, or Google Classroom for pupils to complete and submit for marking and feedback.
- Pre-recorded videos demonstrating specific tasks and supporting pupils' learning when appropriate.
- Additional online materials provided through the school website and Instagram.
- A safety page on the website to signpost online safety resources.
- If only teachers are self-isolating but remain healthy, they will arrange online lessons to deliver class input and maintain contact throughout their isolation period.

Staff Training

- Staff receive regular updates and training on e-Safety issues through annual updates/termly staff meetings, CPD, and emails from the e-Safety Coordinator, as appropriate.
- As part of the induction process, all new staff receive information and guidance on the school's e-Safety Policy and Acceptable Use Policies.
- All staff are informed about their individual responsibilities related to safeguarding children in the context of e-Safety and are aware of what to do if any member of the school community misuses technology.

Incidents

- The school takes all reasonable precautions to ensure online safety.
- Staff and pupils are informed about misuse offenses and potential penalties.
- The e-Safety Coordinator and headteacher are the main points of contact for any incidents.
- The headteacher and e-Safety Coordinator are notified of any suspected online risks or rule breaches.
- Any concerns about staff misuse of equipment are referred directly to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the Chair of Governors.

Data Protection and Information Security

- Personal data will be recorded, processed, transferred, and made available in accordance with the **Data Protection Act 2018**.

- The school employs appropriate technical controls to reduce the risk of data loss or breaches.
- Users must take care when accessing sensitive or personal information on screens to ensure unauthorized individuals cannot read the information.
- Access to all information systems must be managed through suitable complex passwords.
- Staff and pupils must not leave printed personal or sensitive documents on printers in public
- areas of the school.
- All physical information must be stored in controlled-access areas.
- All communication containing personal or sensitive information (email, fax, or post) must be secured appropriately.
- Any personal and sensitive information taken off-site must be protected by appropriate technical controls.
  Devices taken off-site (e.g., laptops, tablets) must be secured following the school's information-handling procedures and must not be left in cars or unsecured locations.

Asset Management

- Details of all hardware owned by the school will be recorded in a hardware inventory.
- All redundant ICT equipment will be disposed of through an authorized agency, and any storage devices potentially containing personal data will be destroyed to prevent recovery.

Monitoring and Review

The school is committed to ensuring this policy has a positive impact on pupils' education, behavior, and well-being. When reviewing the policy, the school will consider:

- Feedback from parents/carers and pupils.
- Feedback from teachers.
- Behaviour and safeguarding incident records.
- Relevant advice from the Department for Education, the local authority, or other relevant organizations.

Appendix 1

CONSENT FORM ALLOWING A PUPIL TO BRING THEIR PHONE TO SCHOOL

PUPIL DETAILS

Pupil's name:
Year group/class:
Parent(s) name(s):

The school has agreed to allow …… to bring [their] mobile phone to school because [he/she]:

- Travels to and from school independently.
- Attends before or after school activities where a mobile phone is needed to contact parents.

By signing this agreement, I agree to adhere to the school's policy on mobile phone use.

I agree to leave my phone in the office in the morning and collect it after leaving the premises at the end of the day.
My phone/device will be switched off and clearly labelled.

I acknowledge that the school accepts no responsibility for mobile phones that are lost, damaged, or stolen on school premises or transport, during school visits or trips, or while pupils travel to and from school.

The school reserves the right to revoke this permission if pupils fail to adhere to the policy.

Parent signature: _____

Pupil signature: _____