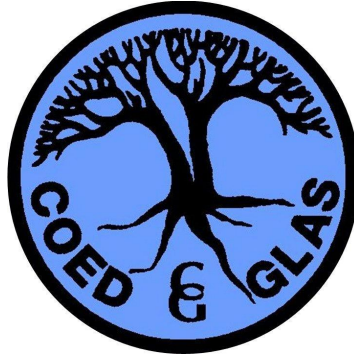


E-SAFETY POLICY

Coed Glas Primary School



Reviewed December 2022

MR. D. CHIN





Contents

Section Title:

1. **Background**
2. **Development / Monitoring / Review**
3. **Scope of the Policy**
4. **Role and Responsibilities**
5. **Education**
6. **Cyber Bullying**
7. **Responding to incidents of misuse**
8. **Social Media – Protecting Professional Integrity and Identity**
9. **Password Security**
10. **Appendices**

Policy Review Dates

Current policy

<i>review date:</i>	Jan 2024		
<i>by:</i>	Mr. David Chin,	<i>E-Learning Coordinator ,</i>	Coed Glas Primary School
<i>approved by:</i>	Miss N Shapley	<i>Safeguarding Officer,</i>	Coed Glas Primary School

Other Notes:

References





1. Background

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

Some of the potential risks could include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to exploitation and abused 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
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence.
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate.
- Risk of sexual exploitation

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

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / 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.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.



2. Development / Monitoring / Review

This e-safety policy has been developed by a Strategic e-Safety working group made up of Headteachers, High School and Primary School ICT Leaders and Local Authority Staff and has been reviewed by a wide range of relevant stakeholders.

Consultation with the whole school community has taken place through a variety of informal and formal meetings.



Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body / Governors Sub Committee on:	Insert date _____
The implementation of this e-safety policy will be monitored by the:	E-Safety Group: E-Learning Coordinator Safeguarding Officer
Monitoring will take place at regular intervals:	Annually in the Autumn Term
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually or as required
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	Annually in the Autumn Term
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA Schools ICT Strategic Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity (school that manage their own filtering)
- Surveys / questionnaires of
- students / pupils (eg CEOP ThinkUknow survey)
- parents / carers
- staff



3. Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, 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 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 regards to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published behaviour policy. 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.



4. Role and Responsibilities



The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

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 / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Coordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and 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 E-Safety Coordinator / Officer (see below).
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- 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 Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Coordinator / Officer.
- The Headteacher and another member of the Senior Leadership Team / Senior Management 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. (see flow chart on dealing with e-safety incidents and online safety incident included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

E-Learning Coordinator:

- leads the e-safety committee
- 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 including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- liaises with the Local Authority
- liaises with ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (see appendix).
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

- TBC

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 school E-Safety Agreement (Adult)
- they report any suspected misuse or problem to the E-Safety Coordinator / Officer / Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction
- all digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be 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 school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations



- they monitor the use of digital technologies, mobile devices, cameras etc in lesson and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-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

Safeguarding Officer should be trained in e-safety issues and be aware of the potential for serious child protection 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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school / academy community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the school / academy this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body / Directors.

Members of the E-safety Group (or other relevant group) will assist the E-Safety Coordinator / Officer (or other relevant person, as above) with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil E-Safety Agreement, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of safe use of digital media and how to report abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

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, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.

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
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed)
- digital media and how to report abuse, misuse or access to inappropriate materials

Visiting Adults and Pupils



Users who access school ICT systems / website / VLE via login as part of the Extended School provision will be expected to sign the appropriate E-Safety Agreement before being provided with access to school systems.



5. Education

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people 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, with opportunities for creative activities and 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 and tutorial / pastoral activities
- Students / 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.
- 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 should be helped to understand the need for the student / pupil E-Safety Agreement 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 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.
- Where students / pupils are allowed to freely search the internet, 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated 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.
- Students should be supported to understand and report unsafe or harmful digital misuse.

Education – parents / 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 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: (select / delete as appropriate)

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education & Training – Staff

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. It is expected that some staff will identify e-safety as a training need within the performance management process.



- 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 Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at Consortium/ LA / other information / training sessions and by reviewing guidance documents released by BECTA / Consortium / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

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 ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents



6. Cyber Bullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period of time. It can often be difficult to gain closure when subject to a cyber bullying incident when the comment or photo can resurface at anytime.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but is **not restricted to**:

- harassment and intimidation of others,
- sending hateful messages,
- posting inappropriate and unwanted pictures online and;
- creating content which has the potential to hurt, embarrass and humiliate others.
- Sexting
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.



7. Responding to incidents of misuse

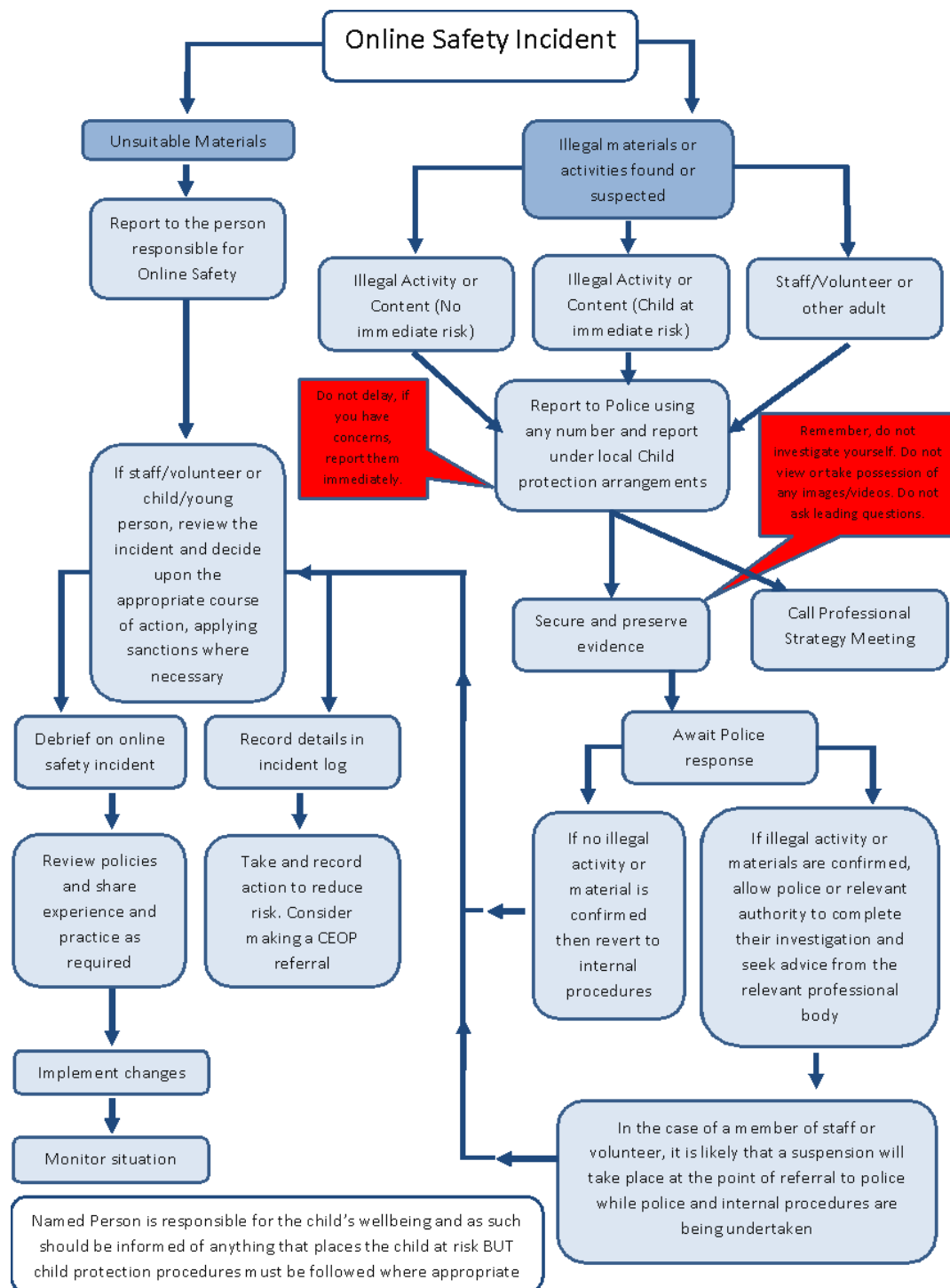


It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out



the investigation. In such event the “Guidance for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed.

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 that follows.



8. Social Media – Protecting Professional Integrity and Identity

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, cyberbully, 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. Reasonable steps to prevent predictable harm must be in place.

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; 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 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the MCR and e-safety group to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.



9. Password Security

The school will be responsible for ensuring that the technology is as safe and secure as is reasonably possible and that: users can only access data to which they have permission, access to personal data is securely controlled in line with the school's personal data policy

Responsibilities

The management of the password security policy will be the responsibility of the e-Safety Co-ordinator. Each user (adults and young people from KS2 onwards) should have their own password and be responsible for its security.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, not written down or shared with anyone else.

Adult users will be made aware of the password policy:

- at induction
- through the E-Safety Agreement

Children / young people will be made aware of the password policy:

- when joining the school
- informally through reminders from staff / volunteers
- through the E-Safety Agreement

Rules for Passwords

- the “master / administrator” passwords for the school should be held by more than one person (including the senior leader), should not be used for day to day use and must be stored securely.



- the master/administrator passwords for the Network, Hwb+ and other VLE's, Google App for Edu and other systems as appropriate will also be kept by the schools E-Learning Co-ordinator
- the password should be a minimum of **6 characters** long and should include a **mixture of characters**
- temporary passwords e.g. users with new user accounts or replacement passwords will be forced to change the temporary password when they next log-on
- there should be an agreed system for requests for password changes.
- where users take laptops with personal data off-site these must be encrypted [marked: **E12345**]



10. Appendices

On the following pages you will find a range of supporting policies:

Management:

- Appendix A.** E-Safety Agreement (Pupil - Foundation Phase)
Appendix B. E-Safety Agreement (Pupil - Key Stage 2)
Appendix C. E-Safety Agreement (Adults)
Appendix D. E-Safety Agreement (Parents)

People:

- Appendix E.** Guidance for reviewing internet sites (for suspected harassment and distress)
Appendix F. Incident reporting log
Appendix G. Training needs audit

Technology:

- Appendix H.** Monitoring log (template)

At the end of this document you will find:

Links to other organisations and documents
Legislation
Glossary
Acknowledgements



End of Policy
