

**Covingham Roundabout Pre-School Ltd**

**E-Safety Policy**

**Development / Monitoring / Review of this Policy**

This E-Safety policy has been developed by Covingham Roundabout Pre-School Ltd.

*• Sarah Randall (Director/Manager)*

*• Paul Randall (Director/E-Safety Officer/Administrato*

**Schedule for Development / Monitoring / Review**

|  |  |
| --- | --- |
| This e-safety policy was approved by Covingham Roundabout Pre-School Ltd | *09/01/2015* |
| The implementation of this e-safety policy will be monitored by: | ***Sarah Randall*** *(Director/Manager)****Paul Randall*** *(Director/E-safety Officer/Administrator)****Maria Hayward*** *(Deputy Manager)* |
| Monitoring will take place at regular intervals: | *Annually from date of approval of policy* |
|  |  |
| 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: | 30/09/2020 |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Paul Randall (Director/E-Safety Officer/Administrator)* |

The school will monitor the impact of the policy using:

*• Logs of reported incidents*

*• Monitoring logs of internet activity (including sites visited)*

*• Surveys / questionnaires of*

*• students / pupils*

*•* parents / carers

*• staff*

**Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school / academy* 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 outside of the Pre-School, but is linked to membership of the Pre-School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Pre-*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 take place out of Pre-School.

**Roles and Responsibilities**

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

**Directors:**

*Directors* 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. A member of the *Directors* has taken on the role of *E-Safety Officer*.

The role of the E-Safety *Officer* will include:

*• Regular meetings with Directors and Deputy Manager*

*• Regular monitoring of e-safety incident logs*

*• Regular monitoring of filtering / change control logs*

*• Reporting to relevant Governors / Board / committee / meeting*

**E-Safety Officer:**

• Leads the e-safety committee

• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Pre-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

• Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with Director and Deputy Manager

• Attends relevant meeting / committee of *Governors / Directors*

• Reports regularly to Senior Leadership Team

**Early Years Staff**

are responsible for ensuring that:

**• They have an up to date awareness of e-safety matters and of the current *Pre-School* e-safety policy and practices**

**• They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**

**• They report any suspected misuse or problem to the *E-Safety Coordinator Officer*****for investigation / action / sanction**

**• All digital communications with students / pupils / parents / carers should be on a professional level** *and only carried out using official Pre-School systems*

**Child Protection/Safeguarding Officers**

**Sarah Randall (Lead)**

**Maria Hayward (Deputy)**

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

**E-Safety Group**

The E-Safety Group provides a consultative group that has wide representation from the Pre-*School* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Directors*.

Members of the *E-safety Group* will assist the *E-Safety Officer* with:

• The production / review / monitoring of the Pre-School e-safety policy / documents.

*•* Mapping andreviewing the e-safety curricular provision – ensuring relevance, breadth and progression

*•* Monitoring network / internet / incident logs

*•* Consulting parents / carers about the e-safety provision

*•* Monitoring improvement actions identified through use of the 360 degree safe self review tool

(Schools / academies will need to decide the membership of the e-safety group. It is recommended that the group should include representation from students / pupils and parents / carers).

An E-Safety Group Terms of Reference Template can be found in the appendices

**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. The *Pre-School* will 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 *Pre-School* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

**•** Digital and video images taken at school events

**Policy Statements**

**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 Pre-School’s e-safety provision. Children and young people need the help and support of the Pre-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:**

**• Key e-safety messages should be reinforced.**

**• Students / pupils should be taught 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**

*• Staff should act as good role models in their use of digital technologies the internet and mobile devices*

*• Where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use*

*• 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.*

**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:

*• Activities*

*• Letters, newsletters, web site, VLE*

*• Parents / Carers evenings*

*• Reference to the relevant web sites / publications eg* [*www.swgfl.org.uk*](http://www.swgfl.org.uk/)[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

**Education & Training – Staff / Volunteers**

It is essential that all staff understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

**• All new staff should receive e-safety policy as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**

*• The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates by reviewing guidance documents released by relevant organisations.*

*• This E-Safety policy and its updates will be presented to staff as a policy document and a signed letter of reciept will be presented to the directors and discussed by staff in staff meetings.*

**Training – Governors / Directors**

**Directors and persons named as part of the e-safety group should take part in e-safety training / awareness sessions**, with particular importance for those who are members of e-safety / child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / or other relevant organisation (eg SWGfL).

• Participation in school training / information sessions for staff

.**Technical – infrastructure / equipment, filtering and monitoring**

The Pre-School will be responsible for ensuring that the 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

**• Pre-School technical systems will be managed in ways that ensure that it meets recommended technical requirements**

• **There will be regular reviews and audits of the safety and security of school academy technical systems**

**• Servers, wireless systems and cabling must be securely located and physical access restricted**

**• All users will have clearly defined access rights to Pre-School technical systems and devices.**

• **Staff** **will be provided with a username and secure password** by *Sarah Randall (manager) Maria Hayward (Deputy Manager) or the e-safety officer Paul Randall who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password every month and provide their updated user name and password to the e-safety officer*

**• The “master / administrator” passwords for the Pre-School , used by the Manager or deputy manager must also be available to the *e-safety officer* and kept in a secure place**

*•* Paul Randall (Director,Administrator,E-safety officer) **is 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**

* **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored

*• Pre-School technical staff regularly monitor and record the activity of users on the school technical systems*

*• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.*

• Appropriate security measures are in place via internet security software to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the Pre-School systems and data. The Pre-School infrastructure and individual workstations are protected by up to date virus software.

• An agreed policy is in place for the provision of temporary access of “guests” (eg trainee/temporary/bank staff and parent helpers) onto the Pre-School systems.

*• An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.*

*• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on Pre-School devices. Personal data cannot be sent over the internet or taken off the Pre-School site unless safely encrypted or otherwise secured.*

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil’s instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

**• When using digital images, staff should inform and educate students / 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 eg on social networking sites.**

•In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). 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.*

• *Care should be taken when taking digital / video images that students / 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*

• *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.*

• *Students’ / 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*

• *Student’s / Pupil’s work can only be published with the permission of the student / pupil and parents or carers.*

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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 Pre-School will ensure**

* **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 in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.**
* It has clear and understood arrangements for the security, storage and transfer of personal data
* Data subjects have rights of access and this can be obtained through the directors

**Staff must ensure that they:**

**• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**

**• Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.**

**• Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

**•** The data must be encrypted and password protected

**•** The device must offer approved virus and malware checking software

**•** The data must be securely deleted from the device once it has been transferred or its use is complete

**Communications**

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

**• The official Pre=*School* email service may be regarded as safe and secure and is monitored.****Users should be aware that email communications are monitored.**

**• Users must immediately report, to the nominated person – in accordance with the school / academy 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 and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official Pre-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 Pre-school website and only official email addresses should be used to identify members of staff.*

**Social Media - Protecting Professional 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, 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.

The Pre-School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Pre-School through limiting access to personal information:

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 Pre-School community
* Personal opinions should not be attributed to the *school /academy* or local authority

The Pre-*School’s* use of social media for professional purposes will be checked regularly by the Directors and e-safety officer

**Unsuitable / inappropriate activities**

The Pre-School believes that the activities referred to in the following section would be inappropriate in a Pre-School context and that users, as defined below, should not engage in these activities in Pre-School or outside Pre-School when using Pre-School equipment or systems. The Pre-School policy restricts usage as follows:

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

**Responding to incidents of misuse**

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

**Illegal Incidents**

**If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.**



**Other Incidents**

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

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

* Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

• Internal response or discipline procedures

• Involvement by Local Authority or national / local organisation (as relevant).

• Police involvement and/or action

* **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
* incidents of ‘grooming’ behaviour
* the sending of obscene materials to a child
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials
* **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

**School / Academy Actions & Sanctions**

It is more likely that the Pre-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 Pre-School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows

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

Every effort has been made to ensure that the information included in this document is

Accurate, as at the date of publication in October 2013. However, Covingham Roundabout Pre-School Ltd cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

**School / Academy Policy**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

• That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

• That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

**Acceptable Use Policy Agreement**

I understand that I must use Pre-School systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

**For my own personal safety:**

• I understand that the Pre-*School* will monitor my use of the systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will be aware of “stranger danger”, when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

**I understand that everyone has equal rights to use technology as a resource and:**

• I understand that the *Pre-School* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not use the Pre-*School* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

**I will act as I expect others to act toward me:**

• I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

**I recognise that the Pre-School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school / academy*:**

• I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission I understand that, if I do use my own devices in the *Pre-School*, I will follow the rules set out in this agreement, in the same way as if I was using Pre-School equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

• I will only use social media sites with permission and at the times that are allowed

**When using the internet for research or recreation, I recognise that:**

• I should ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not try to download copies (including music and videos)

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

• I understand that the *Pre-School* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of Pre-School and where they involve my membership of the Pre-School community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Pre-School network / internet, suspensions, Dismissal, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to Pre-School systems and devices.**

**Parent / Carer Acceptable Use Agreement**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

• That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That Pre-School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Pre-School will try to ensure that *children* will have good access to digital technologies to enhance their learning and will, in return.

Parents are requested to sign the permission form below to show their support of the Pre-School in this important aspect of the Pre-School’s work.

**Permission Form**

Parent / Carers Name

Child's Name

As the parent / carer of the above child, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the Pre-School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the Pre-School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s / daughter’s activity on the ICT systems will be monitored and that the Pre-School will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.

Signed Date

**Use of Digital / Video Images**

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The Pre-School will comply with the Data Protection Act and request parents / carers permission before taking images of members of the Pre-School. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at Pre-School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyones 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.

Parents / carers are requested to sign the permission form below to allow the Pre-School to take and use images of their children and for the parents / carers to agree

**Digital / Video Images Permission Form**

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date

**Staff (and Volunteer) Acceptable Use Policy Agreement**

**Pre-School Policy**

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

**This Acceptable Use Policy is intended to ensure:**

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That Pre-School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• That staff are protected from potential risk in their use of ICT in their everyday work.

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

**Acceptable Use Policy Agreement**

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

**For my professional and personal safety:**

• I understand that the *school / academy* will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school ICT systems (egg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of Pre-School

• I understand that the Pre-School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Pre-School.

• I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

• I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Pre-School’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Pre-School website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use chat and social networking sites in school in accordance with the school’s policies. (schools / academies should amend this section to take account of their policy on access to social networking and similar sites)

• I will only communicate with students / pupils and parents / carers using official pre-school systems. Any such communication will be professional in tone and manner.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

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

• When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will also follow any additional rules set by the *school / academy* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not use personal email addresses on the school ICT systems.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies. (Schools / academies should amend this section in the light of their policies on installing programmes / altering settings)

• I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

• I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

• I understand that this Acceptable Use Policy applies not only to my work and use of school / academy ICT equipment in school, but also applies to my use of school / academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools / academies should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name

Signed

Date

**Responding to incidents of misuse – flow chart**



**Record of reviewing devices / internet sites (responding to incidents of misuse)**

|  |  |
| --- | --- |
| Group | Covingham Roundabout Pre-School Ltd |
| Date |  |
| Reason for investigation |  |

**Details of first reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Details of second reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Name and location of computer used for review (for web sites)**

|  |
| --- |
|  |

**Web site(s) address / device Reason for concern**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Conclusion and Action proposed or taken**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Reporting Log**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Reporting LogGroup .............................................................. | Signature |  |  |  |  |  |  |  |  |
| Incident Reported by |  |  |  |  |  |  |  |  |
| Action taken | By whom? |  |  |  |  |  |  |  |  |
| What? |  |  |  |  |  |  |  |  |
| Incident |  |  |  |  |  |  |  |  |
| Time |  |  |  |  |  |  |  |  |
| Date |  |  |  |  |  |  |  |  |

**Training Needs Audit**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Training Needs Audit LogGroup .............................................................. Date ................................ | Review date |  |  |  |  |  |  |  |  |
| Cost |  |  |  |  |  |  |  |  |
| To be met by: |  |  |  |  |  |  |  |  |
| Identified training need |  |  |  |  |  |  |  |  |
| Relevant trainingin last 12 months |  |  |  |  |  |  |  |  |
| Position |  |  |  |  |  |  |  |  |
| Name |  |  |  |  |  |  |  |  |

**Pre-School Technical Security Policy (including filtering and passwords) - amended January 2015**

**Introduction**

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

• users can only access data to which they have right of access

• no user should be able to access another’s files (other than that allowed for monitoring purposes within the school’s policies).

• access to personal data is securely controlled in line with the school’s personal data policy

• logs are maintained of access by users and of their actions while users of the system

• there is effective guidance and training for users

• there are regular reviews and audits of the safety and security of school computer systems

• there is oversight from senior leaders and these have impact on policy and practice.

**Responsibilities**

The management of technical security will be the responsibility of Sarah Randall (Manager), Maria Hayward (Deputy Manager), Paul Randall (Director, e-safety officer, administrator)

**Technical Security**

**Policy statements**

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 will receive guidance and training and will be effective in carrying out their responsibilities:

**• 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**

**• Appropriate security measures are in place** **to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**

**• Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff**

**• All users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by the Technical Staff and will be reviewed, at least annually, by the E-Safety officer*

*•* Users 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.

*•* Paul Randall (Director,e-safety officer, administrator) is 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

*• Mobile device security and management procedures are in place*

*• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*

*• An appropriate system is in place for users to report any actual / potential technical incident to the E-Safety officer*

• An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system.

*• An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.*

*• The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*

*• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

**Password Security**

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

**Policy Statements**

* All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
* **All school networks and systems will be protected by secure passwords that are regularly changed**
* **The “master / administrator” passwords for the schoolsystems, used by the technical staff must also be available to the senior leader and kept in a secure place e.g. school safe.**
* *Passwords for new users, and replacement passwords for existing users will be allocated by the Manager, Deputy Manager or E-safety officer* *Any changes carried out must be notified to the manager of the password security policy (above).*
* All users (adults and young people) will have responsibility 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.
* *Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below*
* *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

**Staff passwords:**

* **All staff users** **will be provided with a username and password** by *Sarah Randall, Maria Hayward or Paul Randall*
* *the password should be a minimum of 8 characters long and must include at least one upper case character and one number. must not include proper names or any other personal information about the user that might be known by others*

*• Passwords shall not be displayed on screen,*

* *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
* should be changed at least every 60 to 90 days
* Should not re-used for 6 months and be significantly different from previous p *the last four passwords cannot be re-used* passwords created by the same user.
* should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
* should be different for systems used inside and outside of school

**Training / Awareness**

Members of staff will be made aware of the school’s password policy:

• At induction

• Through the school’s e-safety policy and password security policy

• Through the Acceptable Use Agreement

**Audit / Monitoring / Reporting / Review**

The responsible person Sarah Randall Or Maria will ensure that full records are kept of:

• User Ids and requests for password changes

• *User log-ons*

*• Security incidents related to this policy*

**School Personal Data Handling Policy**

.

**Introduction**

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

• have permission to access that data, and/or

• need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office ~~.~~ For the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

**Policy Statements**

The school 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 in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.

**Personal Data**

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

• Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

• Curricular / academic data e.g. class lists, pupil / student progress records, reports, references

• Professional records e.g. employment history, taxation and national insurance records, appraisal records and references

• Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

**Responsibilities**

The school’s Senior Information Risk Officer (SIRO) is Sarah Randall.

 This person will keep up to date with current legislation and guidance and will:

• determine and take responsibility for the school’s information risk policy and risk assessment

• appoint the Information Asset Owners (IAOs)

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

**Registration**

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

**Training & awareness**

All staff will be made aware of their responsibilities, as described in this policy through:

• Induction training for new staff

• Staff meetings / briefings

• Day to day support and guidance relevant persons)

**Secure Storage of and access to data**

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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 (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and

• The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

As a Data Controller, the *school* is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

**Disposal of data**

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

**Relevant legislation:**

* Education Act 1996
* Education and Inspections Act 2006
* Education Act 2011 Part 2 (Discipline)
* The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
* Health and Safety at Work etc. Act 1974
* Obscene Publications Act 1959
* Children Act 1989
* Human Rights Act 1998
* Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

**Responsibilities**

The *Named persons* are responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups.

This policy has been written by and will be reviewed by: Paul Randall (Director,Administrator.E-safety officer)

The *Manager* has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

Sarah Randall (Managing Director, Safeguarding officer)

Paul Randall (Director,Administrator,E-safety officer)

Maria Hayward (Deputy Manager, SENco, Deputy Safeguarding office)

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

**Training / Awareness**

It is essential that all staff should be made aware of and should implement the school’s policy.

Members of staff should be made aware of the school’s policy on "Electronic devices – searching and deletion":

• At induction

• At regular updating sessions on the school’s e-safety policy

**Policy Statements**

**Search:**

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

**Staff** are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

If staff breach these rules:

*The sanctions for breaking these rules can be found in the* sections 1.6 and 1.7 of the policies and procedures held by the Pre-School

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

* Searching with consent - Authorised staff may search with consent for any item.
* Searching without consent - Authorised staff may only search without consent for anything which is either ‘prohibited’ (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

**In carrying out the search:**

The authorised member of staff must have reasonable grounds for suspecting that possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the *person* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *person* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

**Extent of the search:**

**The person conducting the search may not require the *person* to remove any clothing other than outer clothing**.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

‘Possessions’ means any goods over which the person has or appears to have control – this includes desks, lockers and bags.

*A person's* possessions can only be searched in the presence of said person another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

**The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.**

**Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.**

**Electronic devices**

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

**If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:**

* **child sexual abuse images (including images of one child held by another child)**
* **adult material which potentially breaches the Obscene Publications Act**
* **criminally racist material**
* **other criminal conduct, activity or materials**

**Deletion of Data**

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

*A record should be kept of the reasons for the deletion of data / files.*

**Care of Confiscated Devices**

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices

**Audit / Monitoring / Reporting / Review**

The responsible person Sarah Randall will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by Paul Randall... *(E-Safety Officer)* at regular intervals (annually)

This policy will be reviewed by the Directors annually and in response to changes in guidance and evidence gained from the records.

**Legislation**

**Computer Misuse Act 1990**

This Act makes it an offence to:

• Erase or amend data or programs without authority;

• Obtain unauthorised access to a computer;

• “Eavesdrop” on a computer;

• Make unauthorised use of computer time or facilities;

• Maliciously corrupt or erase data or programs;

• Deny access to authorised users.

**Data Protection Act 1998**

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject’s rights.

• Secure.

• Not transferred to other countries without adequate protection.

.

**Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

• Establish the facts;

• Ascertain compliance with regulatory or self-regulatory practices or procedures;

• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

• The school reserves the right to monitor its systems and communications in line with its rights under this act.

**Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

**Telecommunications Act 1984**

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

**The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

**Glossary of terms**

AUP Acceptable Use Policy – see templates earlier in this document

CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPC Child Protection Committee

CPD Continuous Professional Development

CYPS Children and Young Peoples Services (in Local Authorities)

FOSI Family Online Safety Institute

EA Education Authority

ES Education Scotland

HWB Health and Wellbeing

ICO Information Commissioners Office

ICT Information and Communications Technology

ICTMark Quality standard for schools provided by NAACE

INSET In Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers’ Association

IWF Internet Watch Foundation

LA Local Authority

LAN Local Area Network

MIS Management Information System

NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational e-safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

Copyright of the SWGfL School E-Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in November 2013. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.