PRINCE'S MEAD

E-SAFETY POLICY

Author(s):	Andy Walker
Date:	November 2023
Review Frequency:	Annually
Next Review Date:	November 2024
Sub-Committee	Education
Date of Sub-Committee Agreement:	November 2023

Our E-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by the governors.

This policy, supported by the school's acceptable use agreements for staff, governors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school policies listed in the introduction to this policy.

The E-Safety Policy and its implementation will be reviewed annually.

All users need to be aware of the range of risks associated with the use of Internet technologies.

At Prince's Mead, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviors and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies,in and beyond the setting of the classroom.

The school holds personal data on pupils, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for the School to use technology to benefit learners.

Everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy, the Acceptable Use Agreements (for all staff and pupils), Data Protection, Email Protocol and Taking and Storing Images of Children (copies attached) are inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, chromebooks, iPads, webcams, whiteboards, digital video equipment; and technologies owned by pupils and staff, but brought onto school premises (such as laptops and mobile phones).

Roles and responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for e-Safety. Whilst activities of the DSL may be delegated to the appropriately trained deputy DSLs, overall the ultimate lead responsibility for safeguarding and child protection, including e-Safety remains with the DSL. Princes Mead School recognises that all members of the community have important roles and responsibilities to play with regards to e-Safety.

Headteacher and Governing Body

The Headteacher and Governing Body will:

- ensure that e-Safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- ensure there are appropriate and up-to-date policies regarding e-Safety; including a Behaviour Policy, which covers acceptable use of technology
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with I.T support and Sytec to monitor the safety and security of our systems and networks
- ensure that e-Safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of e-Safety

- support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their e-Safety responsibilities
- ensure there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- audit and evaluate e-Safety practice to identify strengths and areas for improvement

Designated Safeguarding Lead (DSL)

The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- work alongside the Deputy DSLs to ensure e-Safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- ensure all members of staff receive regular, up-to-date and appropriate e-Safety training
- access regular and appropriate training and support to ensure they understand the unique risks associated with e-Safety and have the relevant knowledge and up to date required to keep pupils safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online
- keep up-to-date with current research, legislation and trends regarding e-Safety and communicate this with the community, as appropriate
- ensure that e-Safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- maintain records of e-Safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms
- monitor e-Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- report e-Safety concerns, as appropriate, to the Leadership Team and Governing Body
- work with the Leadership Team to review and update e-Safety policies on a regular basis (at least annually) with stakeholder input
- meet annually with the governor with a lead responsibility for safeguarding and online safety

Staff Members

It is the responsibility of all members of staff to:

- contribute to the development of e-Safety policies
- read and adhere to the e-Safety policy and acceptable use policies
- take responsibility for the security of school systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- embed e-Safety education in curriculum delivery, wherever possible
- have an awareness of a range of e-Safety issues and how they may be experienced by the pupils in their care
- identify e-Safety concerns and take appropriate action by following the school's safeguarding policies and procedures
- know when and how to escalate e-Safety issues, including signposting to appropriate support, internally and externally
- take personal responsibility for professional development in this area

It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate e-Safety policies and procedures

- implement appropriate security measures as directed by the DSL and Leadership Team, such as password policies and encryption, to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure that the monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- ensure appropriate access and technical support is given to the DSL and the Deputy DSLs to the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required

Pupils

It is the responsibility of pupils (at a level appropriate to their age and ability) to:

- engage in age appropriate e-Safety education opportunities
- read and adhere to the acceptable use policies
- respect the feelings and rights of others both on and offline
- take responsibility for keeping themselves and others safe online
- seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-Safety issues

Parents/Carers

It is the responsibility of parents/carers to:

- read the acceptable use policies and encourage their children to adhere to them
- support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- contribute to the development of the e-Safety policies
- use school systems, such as learning platforms, and other network resources, safely and Appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Education and Engagement with Pupils

Prince's Mead school will establish and embed a progressive e-Safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring education regarding safe and responsible use precedes internet access
- including e-Safety in Learning for life lessons, Relationships and Sex Education (RSE) and digital literacy programmes of study
- reinforcing e-Safety messages whenever technology or the internet is in use
- educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Teaching and Learning

Why Internet use is important?

The Internet is an essential element in 21st century life for education, business and social interaction.

The school has a duty to provide students and staff with quality Internet access as part of their teaching and learning experience.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and vlogs
- Podcasting
- Video Broadcasting/Streaming
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Internet use will enhance learning

The school Internet access has been designed expressly for pupil and staff use and will include monitoring for staff and pupils and filtering for staff and appropriate filtering to the age of pupils.

Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use by formal E-safety lessons taught by the Head of Digital learning and by staff in their Learning for life lessons. Other learning opportunties for E Safety are reinforced when technology is used in other subject areas.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Reducing online risks

Prince's Mead School recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.
We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the school's computers or devices.
All members of the community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the acceptable use policies and highlighted through a variety of education and training approaches.

Managing Internet Access

Information system security;

- School computer systems capacity and security will be reviewed regularly.
- Firewall protection will be updated regularly.

Email;

Pupils do have email accounts on the school system via microsfot 365 but learn about e-safety through e-safety activities in digitallearning lessons in a controlled environment.

Publishing pupil's images and work

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

Staff must refer to the image consent list of children who can be photographed for use on our school website or outside publications before taking photographs.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

A copy of the Taking and Storing of Images of Children is attached to this policy.

Social networking

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school uses Impero Web Security filtering to ensure the systems are filtered appropriately, effectively and reasonably.

If staff or pupils discover an unsuitable site, it must be reported to our I.T support team; support@trailblazeit.co.uk or the Head of Digital learning; andrew.walker@princesmeadschool.org.uk immediately.

The Head of Digital learning will ensure that termly checks are made to ensure that the filtering methods are appropriate, effective and reasonable.

Viruses and malware

Pupils and Staff using personal removable media are responsible for measures to protect against viruses, making sure the devices have up-to-date virus protection software. It is not the School's

responsibility or that of the I.T Department, to install or maintain virus protection on personal systems.

Pupils and staff are not permitted to download programs on school based technologies. If there are any issues related to viruses or anti-virus software, I.T Support should be informed immediately.

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If you suspect there may be a virus on any school ICT equipment contact the ICT department immediately. They will advise you what actions to take and be responsible for advising others that need to know.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will not be used by pupils at Prince's Mead.

Protecting personal data

Accessing and appropriate use of school data is something that the school takes very seriously. The school follows the Data Protection Act 1998 Guidelines. The School gives relevant staff access to its Management Information System, with a unique ID and password. It is the responsibility of everyone to keep passwords secure. Staff have been issued with the following policies: Acceptable Use, Email Protocol, Data Protection and Taking, Storing and Using Images of Children. The acceptable use policy is given to staff to sign each new year.

The school holds personal data on pupils, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual.

The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for the School to use technology to benefit learners.

The School has appointed the Bursar as Data Protection Officer (DPO) .

Everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, scan and copiers) are used.

Both this policy, the Acceptable Use Agreements (for all staff and pupils), Data Protection, Email Protocol and Taking and Storing Images of Children (copies attached) are inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, chromebooks, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops and mobile phones).

Remote access

Staff are responsible for all activity via your laptop and 365 account.

Only use equipment with an appropriate level of security for remote access.

Avoid writing down or otherwise recording any network access information. Any information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

At Pre Prep, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return an online acceptable use form.

Monitoring

The school uses Impero Internet Monitoring and Reporting to monitor all internet use. Authorised staff will inspect the logs more closely if an alert is created. Any ICT equipment owned or leased by the School can at any time without prior notice be checked. If you are in doubt as to whether the individual requesting such access is authorised to do so, please consult with the Head Master .

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without prior consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime. If such action is carried out, the date and time of access will be recorded, along with a reason for doing so.

ICT authorised staff may, without prior notice, access the e-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the

Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that all communications using the School's network could be intercepted, monitored or recorded, this could involve personal communications conducted using School infrastructure.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept liability for the material accessed, or any consequences of Internet access.

All users are made aware of the procedures for reporting accidental access to inappropriate materials. This must be immediately reported to the ICT department. Deliberate access to

inappropriate materials by any user will lead to the incident being logged by the E safety Officer, depending on the seriousness of the offence; investigation by Headmaster, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

The school will audit ICT provision to establish if the E-safety policy is adequate and that its implementation is effective and robust.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by the Headmaster.

Any complaint about staff misuse must be referred to the Headmaster.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to the schools DSL, Mr Alex Greenaway.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Roles and Reponsibilities

As e-safety is an important aspect of strategic leadership within the school, the Headmaster and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety officer at Prince's Mead is Alex Greenaway, Deputy Head Master. All members of the school community have been made aware of who holds this post.

This policy, supported by the school's acceptable use agreements for staff, governors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school policies listed in the introduction to this policy.

Introducing the E-safety policy to pupils

Digital learning and online resources are increasingly used across the curriculum. The School believe it is essential for e-safety guidance to be given to the pupils on a regular basis. e-safety lessons are embedded within our curriculum.

Educating pupils on the dangers of technologies that may be encountered outside school is taught as part of the e-safety curriculum bothin digital learning lessons and through the school's "learning for life" PSHE curriculum as well as being reinforced informally on a regular basis.

Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

Pupils are taught to evaluate materials and learn good searching skills, discussions and via the digital learning curriculum.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Staff and the e-Safety policy

New staff receive information on the school's acceptable use policy and email protocol as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).

All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

All staff will be given the School E-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy on the school Web site.

Social media

Expectations
The expectations regarding safe and responsible use of social media applies to all members of the Princes Mead School community.
The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
All members of the Princes Mead School community are expected to engage in social media in a positive, safe and responsible manner.
All members of the Princes Mead School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that maybe considered threatening, hurtful or defamatory to others.
Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
Concerns regarding the online conduct of any member of the Princes Mead School community on social media, should be reported to the DSL and will be managed in accordance with our Child Protection Policy for Managing Allegations against Staff, Anti-bullying, Behaviour and Safeguarding Policies.

Staff Personal Use of Social Media
The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies.

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
All members of staff are advised to safeguard themselves and their privacy when using social media sites.
Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
• Setting the privacy levels of their personal sites
• Being aware of location sharing services

• Opting out of public listings on social networking sites
• Logging out of accounts after use
• Keeping passwords safe and confidential
• Ensuring staff do not represent their personal views as that of the school

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework. Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL and/or the Headmaster immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with pupils and parents/carers
All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL and/or the Headmaster.
If ongoing contact with pupils is required once they have left the school, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL and/or the Headteacher.
Any communication from pupils and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as mobile phones, gaming devices, are familiar to children outside of school too.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

The school allows staff to bring in personal mobile phones and devices for their own use. Members of EYFS must ensure that devices are locked away when on site. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device unless it is for the purpose of enhancing their duties.

Each class/classroom has it's own iPad, this is to be used for school based tasks only inlcuding taking pictures and videos of evidence of good work for display and assessment purposes. If their iPad is unavaiable at a particular time, staff may be allowed to use their own phone to record evidence for these purposes. The images/videos must be uploaded to the school server BEFORE THE END OF THE DAY and deleted from their own device as well.

The school publishes the Staff/Pupils' rules for shared teams/documents and emails, for children to see, as detailed here:

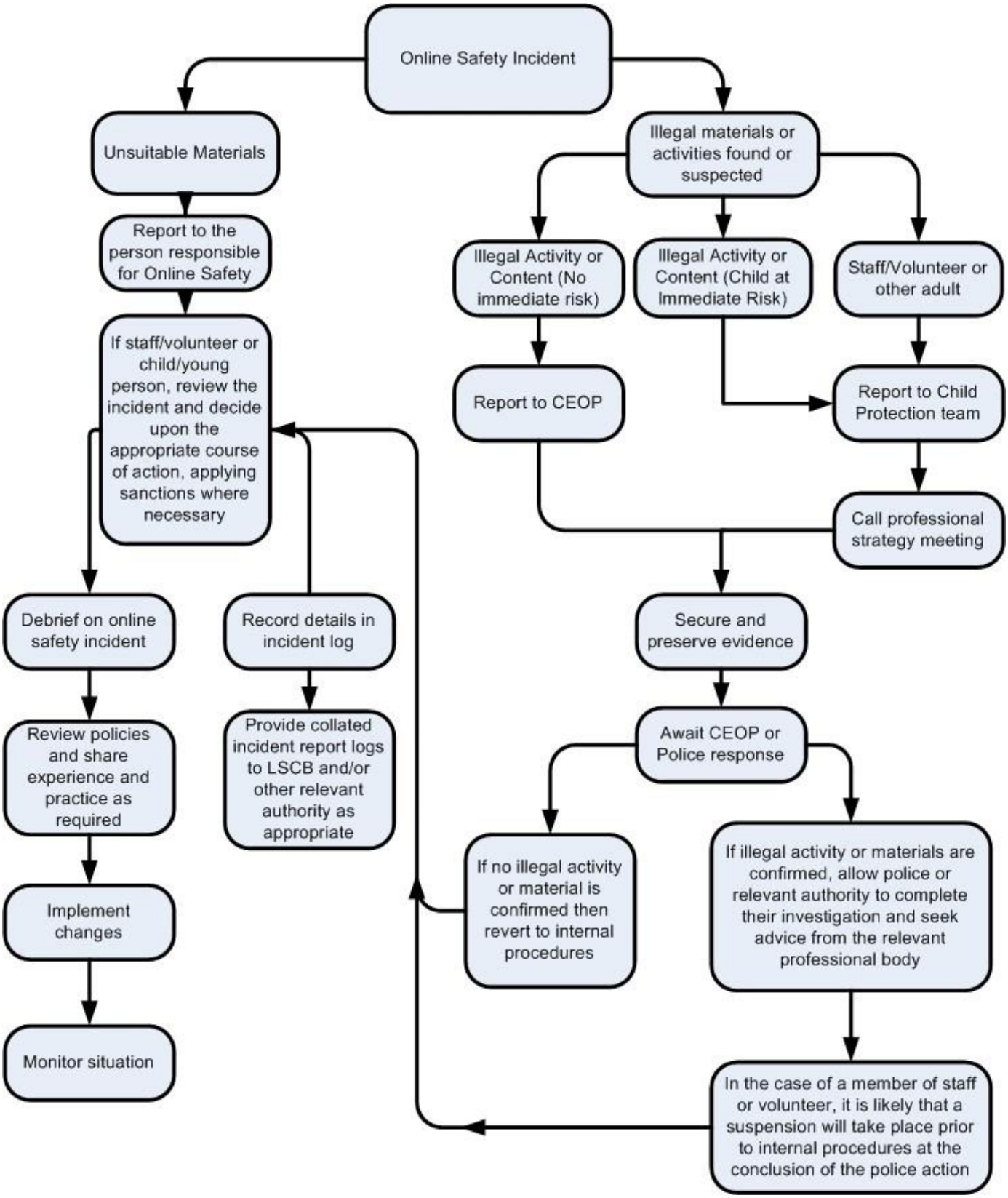
- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate messages/images between any member of the school community is not allowed.
- Staff should not be found to be storing images of school pupils anywhere on their personal devices. Exceptions may be made for mobile devices that are used solely for the purpose of work and it will be up to the owner of the device to prove this; images must be deleted that day once uploaded to the system.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Members of aurthorised ICT staff, the Headmaster, Deputy headmaster (DSL) have the right, in the interests of Child Protection, to perform spot checks, on any mobile phone or device that is present on school premises, with the owner present.

Appendices:

1. Responding to incidents of misuse – flow chart
2. Example of record for reviewing devices
3. Taking, storing and using images of children policy
4. Data Protection policy
5. Staff acceptable use agreement
6. Staff Advice ICT Do and don’ts Checklist
7. Pupil/parent acceptable use agreement

1. Responding to incidents of misuse – flow chart



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

Group	
Date	
Smoothwall Instant Notification – Category	

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

3. Taking, storing and using images of children policy

At Prince's Mead School, we are an open and inclusive community that is very proud of all of the achievements of all of our pupils in their academic, artistic and sporting endeavours. We celebrate our diversity and give all of our many visitors a warm welcome.

We particularly welcome parents to our concerts, plays and sporting events, as well as to more formal occasions during the school year. The school walls are decorated with examples of pupils' work, team photographs and photographs of trips and expeditions in which our pupils have participated. We make full use of electronic notice boards inside the school to enhance our displays. Our web site is updated regularly, and all parents are sent our weekly newsletter, The Link, in order to keep them fully abreast with the news of our active community.

The Application of Data Protection Laws to Taking, Using and Storing Images of Children

Parents who accept a place for their child at Prince's Mead School are invited to agree to the school using anonymous photographs of their child and information relating to his or her achievements for promotional purposes, which may be published in the prospectus or on the web site, as well as displayed within the premises, and in bulletins sent to the school community.

Use of Images: Displays etc.

We will only use images of our pupils for the following purposes:

Internal displays (including clips of moving images) on digital and conventional notice boards within the school premises,

Marketing the school both digitally by web site, by prospectus [which includes a DVD], by displays at educational fairs and other marketing functions and by other means.

Use of Images: Internal Identification

All pupils are photographed on entering the school and, thereafter, annually, for the purposes of internal identification.

These passport-sized photographs identify the pupil by:

Name

Year Group

House

They are securely stored in the password-protected area of the school database, where access is restricted to academic, pastoral and school office staff. Any parent who so requests will be sent a copy of his or her son or daughter's photograph.

Use of Images: Internal Identification

A learning journal will be used to reflect your child's time in Reception. It will include photographs of your child at work and play including them with other children at times. These images are stored in a secure on-line server known as 'Tapestry'.

Images that we use in Displays and on our Website

The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, " football team, Spring Term 2022"). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit the school. Parents are given the opportunity to purchase copies of these photographs.

Storage and Review

Our images are securely either in locked filing cabinets, or in a password protected section of the school's database. They are reviewed annually and are deleted when no longer required, or when a pupil leaves Prince's Mead School.

We have a procedure in place for regularly checking and updating our web site, when expired material is deleted. We follow Government guidance on e-safety.

Media Coverage

We will always notify parents in advance when we expect the press to attend an event in which our pupils are participating, and will make every effort to ensure that children whose parents or guardians have refused permission for images of their children to be used are excluded from the event.

We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the children of celebrities.

Staff Induction

All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of children.

Use of Cameras and Recording Equipment by Parents and Guardians

Parents are welcome to take photographs of their own children taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.

When taking photographs of the children at Prince's Mead, it is not permitted to publish those images or videos on the Internet e.g. on social networking sites.

We ask parents not to take photographs of other pupils on their own, without the prior agreement of that child's parents.

Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events.

Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply.

Treating others with respect

Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying policy is available on request. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issue to a member of the pastoral staff.

Child's Full Name: _____ Date of Birth: _____

Image Consent Form – Photography and Use of Images or Recordings of Children

I/we have read the School's policy on taking, using and storing of images of children, and I/we agree to that:

The School may use our child's image/recording on internal display boards (both digital and conventional) within the School.	Yes / No (delete as appropriate)
The School may use our child's image in material that is sent both electronically and by paper to the School Community (parents, pupils, staff, Governors and alumni).	Yes / No (delete as appropriate)
The School may use our child's image in printed material that is sent to prospective parents.	Yes / No (delete as appropriate)
The School may use our child's image/recording on its website and on marketing material.	Yes / No (delete as appropriate)

This Consent Form is valid for:

The duration of our child's time at the School	Yes / No (delete as appropriate)
Shorter time – please specify	

I/we understand that the School will always try to contact us in advance when a visit by the media is expected.

I/we understand that I/we may revoke or amend this consent at anytime by giving written notice to the School.

I/we agree to adhere to the School's guidelines for the private use of cameras and recording equipment.

Signature of parent: _____

Or Guardian: _____

Date: _____

4. Data protection policy

General Statement of the School's Duties

The School is required to process relevant personal data regarding workers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller

The School has appointed The Bursar as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998.

The Principles

The School shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

Fairly and lawfully processed

Processed for a lawful purpose

Adequate, relevant and not excessive

Accurate and up to date

Not kept for longer than necessary

Processed in accordance with the data subject's rights

Secure

Not transferred to other countries without adequate protection

Personal Data

Personal data covers both facts and opinions about an individual. It includes information necessary for employment such as the worker's name and address and details for payment of salary.

Processing of Personal Data

A worker's consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the worker.

Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding a worker. Sensitive personal data includes medical information and data relating to gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the worker will generally be required in writing.

Rights of Access to Information

Workers have the right of access to information held by the School, subject to the provisions of the Data Protection Act 1998. Any worker wishing to access their personal data should put their request in writing to the DPO. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to

provide a reply to an access to information request. The information will be imparted to the worker as soon as is reasonably possible after it has come to the School's attention.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

The prevention or detection of crime;

The assessment of any tax or duty;

Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

Accuracy

The School will endeavour to ensure that all personal data held in relation to workers is accurate. Workers must notify the DPO of any changes to information held about them. A worker has the right to request that inaccurate information about them is erased.

Enforcement

If a worker believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the worker should utilise the School grievance procedure and should also notify the DPO.

Data Security

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to both staff and pupils. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar. Where a worker is permitted to take data offsite it will need to be encrypted.

5. Staff acceptable use policy – this document is now an online Google document; the following is a copy

Please note that this document forms part of your terms and conditions of employment.

Prince's Mead School (The School) uses various Information Communications Technology (ICT) systems to support school operations. ICT systems represent a significant investment and it is in the interests of employees and The School that systems are not subject to malicious, accidental or unintentional abuse or damage.

What constitutes acceptable and unacceptable use of systems is not limited to the statements within this document and personnel granted access to ICT systems owned by The School are urged to maintain a co-operative and common sense attitude in accepting and applying this policy.

Any questions regarding this policy document or ICT system use should be directed to I.T support or the Head of digital learning. Any employee who feels they do not have sufficient knowledge or skills to comply with this policy must inform the Head of digital learning.

Terms

'The School' refers to Prince's Mead School.

'System Administrator' refers to the individual/s charged by The School to take responsibility of the operation and upkeep of ICT systems.

'Information Communications Technology systems', 'ICT systems' and 'School Network' refer to any technology device, owned or used by The School, including but not limited to;

Desktop PCs

Laptops

Servers

Mobile devices

Any device or peripheral directly or indirectly connected to a device listed above

Any piece of software used by any device listed above

Purpose

The School provides ICT systems for the use of employees in support of their day to day duties and responsibilities in delivering the children's education at The School.

Acceptable Use

ICT systems may be used for the following purposes;

The day to day operation of The School

Activities that enhance The School's ability to provide education to its children

Activities that reduce the cost of providing education to The School's children

Activities that enhance The School's ability to achieve its stated mission goals.

Unacceptable Use of IT Systems and Social Media

Unacceptable use of ICT systems internal and external of school includes but is not limited to the following:

I agree that I will not take part or be party to:

Any activity not connected with or in the interests of The School unless specifically sanctioned in writing by the Head.

Any activity pertaining to any commercial enterprise other than The School's.

Any activity that may harm The School's reputation to any other individual or organisation.

Accessing, blogging, posting or uploading on Social Networking Sites or online dating sites including but not limited to: Facebook, Twitter, You Tube, Instagram, E-Harmony etc unless relating to school business and with given permission from the Head.

I will not allow existing parents to add me as a friend, nor will I add them as friends, on social networking sites.

I will not allow past pupils to add me as a friend, nor will I add them as friends until they are 18 years of age.

I must make clear that any comments (e.g. political views) are my own personal opinion.

I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school into disrepute.

In line with safeguarding procedures, no comments should be made with reference to the school, its staff, governors, pupils, families, any persons associated with it or events.

I will not place any information regarding my activities at school, or the school in general on my social networking sites.

Any activity that may harm the reputation of any individual or organisation.

I will not contact pupils via email or accept or respond to emails from pupils accept through the use of Teams for the purpose of hybrid learning when necessary.

Any activity that increases the cost of maintenance and support of ICT systems and which is subsequently judged unacceptable by the System Administrator or the Governors of The School.

Any activity that is illegal.

Violating software and material copyrights or intellectual property rights.

Malicious damage to hardware, software or other materials.

Communicating offensive, threatening or abusive language or material.

Modifying or deleting computer software or data on the ICT systems without authority.

Knowingly using harmful software.

Access , copy, remove or otherwise alter any other user's files without their express permission.

Responsibilities

Any employee using The School's ICT Systems for storing, transferring or accessing any material that may be deemed illegal or obscene within the United Kingdom will be reported to the Police. Further The School shall provide the Police with any material evidence required to aid the Police in securing a prosecution.

An employee is deemed to be an authorised ICT System user on issue of a user id and password.

Only authorised (all academic, support and administrative staff) users may access The School's ICT systems.

Authorised users may not disclose their user id and password to any other individual unless specifically sanctioned to do so by the Head or the System Administrator.

Where a user believes or suspects that their password has become known to another individual they should change their password at the earliest opportunity.

Where a user is aware that a password has become known to an unauthorised person they must inform the System Administrator at the earliest opportunity.

Authorised users may only access programs and data that they require for the successful completion of their day to day duties and responsibilities.

Any employee who is made aware of a security breach on ICT Systems must report such a breach to the System Administrator at the earliest opportunity.

Any employee who is made aware of any security loophole that exposes data to unauthorised users must report such a loophole to the System Administrator at the earliest opportunity.

All users must ensure that they log out of systems or lock when leaving them unattended for whatever reason. No system should be left in a state where an unauthorised individual may gain access. The system must be turned off or left in a state where a password is required prior to further use.

Specific Responsibilities

Data Files

Data files constitute files that can not be easily reconstructed in the event of a system failure. For instance, a program such as Word may easily be re-installed, however the .DOC files produced by Word may not be easily constructed.

All users must save files pertinent to The School in network drives for daily backup and/or the cloud drive.

No user may delete a file they are not responsible for.

Users accept that the System Administrator may remove any particular system from any user at any time. For this reason all data files must be stored on network servers.

Network Passwords

It will need to be a minimum of 8 characters with one number, one upper case letter and one special character.

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can be incorporated as needed, for example 3redHousemonkeys27!

Be creative and use words memorable to you, so that people can't guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess.

Cyber criminals are very smart and know many of the simple substitutions we use such as 'Pa55word!" which utilises symbols to replace letters.

Never use the following personal details for your password:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

E-safety

I understand that it is my duty to promote e-Safety with children in my care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner.

I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing

I will report any incidents of concern regarding children's safety to the Deputy Headmaster (DSL)

Removable media

Removable media can only be used in extreme circumstances, for example if our school Dashboard is down. Removable media must be virus checked before being used in The School's ICT systems.

All staff are to ensure that any removable media is free of viruses or malicious software. This is the responsibility of the staff who must have anti virus software on all personal computers.

Software

Only software installed by the System Administrator (or representative) may be used.

Users who would like to use software not already installed should submit a request to the ICT department for testing its compatibility on the School's network and written justification as to how and why the software would benefit The School. The System Administrator will inform the user of any decision made and include a brief supporting statement.

Under no circumstances should a program file, specifically files with a .EXE .COM .BAT .PIF .SCR extension, be downloaded from the Internet or any other external information system.

Games may not be used under any circumstances unless previously installed by the System Administrator.

Personal Use

- The School does not discourage the use of ICT Systems for personal use as long as such use is not in contravention of this policy and does not in any way increase The School's costs. The school alows users to bring in personal mobile devices.

ICT systems may not be used for personal use within working hours. Please refer to Unacceptable Use in this policy.

Personal e-mail message must not include binary attachments greater than 5Mb.

The total size of personal files must not be greater than 1Mb for any individual.

Personal files must be kept in the user folder allocated.

Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device unless it is for the purpose of enhancing their duties.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Staff should not be found to be storing images of school pupils anywhere on their personal devices. Exceptions may be made for mobile devices that are used solely for the purpose of work and it will be up to the owner of the device to prove this.

Legislation

There are several Acts of Parliament which govern the way we may use computers:

The Computer Misuse Act, 1990

This act states that you may not make unauthorised access, or modifications to computer material.

The Copyright Design and Patents Act, 1988

This act forbids the unauthorised copying of computer programmes. It also makes it an offence to use, distribute or permit the use of unauthorised copies.

The Data Protection Act, 2018

- **This Act makes provision about the processing of personal data. Most processing of personal data is subject to the GDPR. Makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive. It also makes provision about the enforcement of the data protection legislation.**

Staff are asked to sign this form and return to the Headmaster.

Member of Staff

As a user of the school network, school e-mail and of the Internet, I agree to the school rules on their use. I will use the Internet in a responsible way and observe all the restrictions explained to me by the school. I will tell the Headmaster or the ICT Coordinator immediately if I think I may have accidentally done something to the network or if I have found a web site that is unsuitable. I understand that the school filters Internet access for offensive and inappropriate material, to ensure compliance with the law, this code and other purposes. I understand that the School will monitor mine more closely if it is suspected that I am breaking the rules of acceptable use.

Name of Staff Member: _____

Staff Signature: _____

Date: _____

7. Use of ICT: Do's and Don'ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff, both in and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General Issues

Do:

ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources

ensure that where a password is required for access to a system, that it is not inappropriately disclosed

respect copyright and intellectual property rights

ensure that you have approval for any personal use of the school's ICT resources and facilities

be aware that the school's systems will be monitored and recorded to ensure policy compliance

ensure you comply with the requirements of the Data Protection Act when using personal data

seek approval before taking personal data off the school site

ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely

report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Head (DSL) or designated manager as appropriate

be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal

ensure that any equipment provided for use at home is not accessed by anyone not approved to use it

ensure that you have received adequate training in ICT

ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't:

access or use any systems, resources or equipment without being sure that you have permission to do so

access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for

compromise any confidentiality requirements in relation to material and resources accessed through ICT systems

use systems, resources or equipment for personal use without having approval to do so

use other people's log on and password details to access school systems and resources

download, upload or install any hardware or software without approval

use unsecure removable storage devices to store personal data

use school systems for personal financial gain, gambling, political activity or advertising

Use of Email, the Internet, VLE's and School Intranets

Do:

alert your Head of Digitasl learning or I.T support if you receive inappropriate content via email

be aware that the school's email system will be monitored and recorded to ensure policy compliance

ensure that your email communications are compatible with your professional role

give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate

be aware that the school may intercept emails where it believes that there is inappropriate use

seek support to block spam

alert your Head of ICT if you accidentally access a website with inappropriate content

answer email messages from parents within your directed time or at your convenience

Don't:

send via email or download from email, any inappropriate content

send messages that could be misinterpreted or misunderstood

use personal email addresses to communicate with pupils or parents

send messages in the heat of the moment

send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude

use email systems to communicate with parents or pupils unless approved to do so

download attachments from emails without being sure of the security and content of the attachment

forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention

access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school intranet

Use of Telephones, Mobile Telephones and Instant Messaging

Do:

ensure that your communications are compatible with your professional role

ensure that you comply with your school's policy on use of personal mobile telephones

ensure that you reimburse your school for personal telephone calls as required

use school mobile telephones if possible when on educational visits

Don't:

send messages that could be misinterpreted or misunderstood

excessively use the school's telephone system for personal calls

use personal or school mobile telephones when driving

use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of Cameras and Recording Equipment

Do:

ensure that material recorded is for educational purposes only

ensure that where recording equipment is to be used, approval has been given to do so

ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy

ensure that parental consent has been given before you take pictures of school pupils

Don't:

bring personal recording equipment into school without the prior approval of the Head

inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded

put material onto the VLE or school intranet without prior agreement from the appropriate ICT manager

Use of Social Networking Sites

Do:

ensure that you understand how any site you use operates and therefore the risks associated with using the site

familiarise yourself with the processes for reporting misuse of the site

consider carefully who you accept as friends on a social networking site

report to your Head any incidents where a pupil has sought to become your friend through a social networking site

take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain

ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page

follow school procedures for contacting parents and/or pupils

only contact pupils and/or parents via school based computer systems

through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't:

use social networking sites while at work

accept friendship requests from pupils or parents – you may be giving them access to personal information, and allowing them to contact you inappropriately

put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial

post anything that may be interpreted as slanderous towards colleagues, pupils or parents

use social networking sites to contact parents and/or pupils

8. Acceptable use policy for pupils and parents – this is now an online Google form and will be sent to any new parent – the following is a copy of that form

This is the acceptable usage policy for our School, Prince's Mead. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully and sign at the bottom to show you agree with these terms. If you do not sign and return this form you will not be able to use the school's IT systems.

Pupils in Reception – Year 2 are not required to sign this agreement but we ask a parent or guardian to sign on their behalf as this agreement is for their entire time at Prince's Mead.

For Pupils:

I will only use the School Internet and network for my school work or when a teacher has given me permission.

I will not share my Internet or network passwords.

I will not look at or delete other people's work or files.

I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils or teachers.

I won't search for inappropriate websites. I will check with a teacher if I think a website is unsuitable.

I won't give out my personal details, such as my name, address, school or phone number on the Internet.

I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.

I will be careful with laptops, tablets, mice, keyboards, headphones and all other equipment and when logging on and shutting down a computer.

I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.

I will try to follow these rules all the time because I know they are designed to keep me safe.

Images of pupils will only be taken, stored and used for school purposes in line with the school policy.

Signed Pupil: _____

For Parents:

I understand that it is the responsibility of parents/carers to:

- read the acceptable use policies and encourage their children to adhere to them
- support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online

- use school systems, such as learning platforms, and other network resources, safely and appropriately.

I agree to support and upload the principles of this policy in relation to my child and their use of the Internet at home and at school.

I agree to support and uphold the principles in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school. In the event of any offensive or inappropriate comments being made, I will be asked by the school to remove the post and I will be invited to discuss the issues in person.

Signed Parent/Guardian: _____

Date: _____