E-Safety Policy

The Dormston School recognises that the use of information and communication technologies in school brings a great advantage to the school, but we recognise that E-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

This policy applies to all pupils, employees of the school, the governing body, volunteers, visitors and members of the public on school grounds.

E-safety continues to be a key priority for the Dormston School. The whole school has a consistent approach to e-safety. We ensure that all teaching and non-teaching staff can recognise and be aware of e-safety issues and that the senior management team make it a priority across all areas of school, there is a commitment to training, the development of policies and a straight forward consistent approach when tackling an incident.

E-safety is not about technology but about people and their actions.

Due to the high rate of change this policy will be reviewed and updated on an annual basis.

Responsible Officer – Mr S Carroll
Review Officer – Mr N Eveson
Link Governor – Mr T Proctor
Review Date: December 2018

Contents

1. Why does the school need an E-Safety policy?

In today's society, children young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

The internet and email play an essential role in the conduct of our business in school. The systems within school are made available to pupils, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment within the school in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

E-safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education for all members of the schools community on risks and responsibilities and is part of our 'Duty of Care' which applies to everyone working with children. How we communicate with people not only reflects on us as individuals but on the school. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of email and the internet.

We as a School must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating pupils and staff about responsible use. We must be aware that children and staff cannot be completely prevented from being exposed to risks both off and on line. We believe that children should be empowered and educated so they feel equipped with the skills needed to make safe and responsible decisions as well as to report any concerns.

All members of staff will have training and updates to be aware of the importance of good e-safety practice in the classroom in order to educate and protect pupils in their care. Members of staff will also be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible to their role. We trust staff to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues in accordance with this policy.

Breaches of e-safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all staff are aware of the offline consequences that online actions can have.

We as a School are aware of the legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head teacher and the governing body.

This policy is essential in setting out the schools core principles for e-safety which all members of the school community need to be aware of and understand.

It is important that we all see this as a whole school issue. As such we must all play our part in embedding safe practice.

This policy applies to you as an employee whatever your position. Any inappropriate use of the schools internet & email systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

2. Who will write and review this policy?

As recommended in best practice the school has appointed an e-safety coordinator to lead on e-safety. The schools e-safety policy and its implementation will be reviewed annually. Our e-safety policy has been written by the school based upon the Dudley Council e-safety policy and government guidance.

School E-safety Coordinator: Mr Simon Carroll (Deputy Head)

School E-safety deputy Coordinator: Mr Neil Eveson (School Business Manager)

School Senior Information Risk Owner (SIRO): Mr Ben Stitchman (Head Teacher)

E-safety Governor: Mr Tony Proctor

Policy approved by Head Teacher: September 2016

Policy approved by Governing Body: September 2016

Date of next review is: September 2017 (or earlier if necessary)

3. Why is internet use important?

The internet is part of the everyday life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

Pupils use the internet widely outside of school and need to learn how to evaluate internet information and to take care of their own safety and security.

The purpose of internet use in school is to raise educational standards, to promote pupils, achievement, to support the professional work of staff and to enhance the schools management functions.

Internet access is an entitlement for pupils who show a responsibility and mature approach to its use.

We trust you use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the ip address) can be logged by the site you visit, thus identifying your school.

4. How does the internet benefit education?

Benefits of using the internet in education include:

- ✓ access to worldwide educational resources;
- ✓ inclusion in the National Education Network which connects all schools;
- ✓ educational and cultural exchanges between pupils worldwide;
- ✓ vocational, social and leisure use in clubs and at home;
- ✓ access to experts in many fields for pupils and staff;
- ✓ professional development for staff;
- ✓ collaboration across networks of schools, support services and professional associations;
- ✓ improved access to technical support including remote management of networks and automatic system updates;
- ✓ exchange of curriculum and administration data with DfE;
- ✓ access to learning wherever and whenever convenient;
- ✓ provides routes to access and disseminate information.

5. How can internet use enhance learning?

- ✓ pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use;

- ✓ access levels of the internet will be reviewed to reflect curriculum requirements and the age and ability of the pupils. This will be constantly and consistently monitored;
- ✓ the school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law;
- ✓ staff will guide pupils to online activities that will support the learning outcomes planned for the pupil's age and ability.

6. How will pupils learn how to evaluate internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the internet or email or text messages requires even better information handling and digital literacy skills.

- ✓ pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- ✓ the evaluation of online materials is part of teaching and learning in every subject and will be viewed as a whole-school requirement across curriculum.
- ✓ This is covered in the Pupil Acceptable Use Policy statement.

7. Reporting Routines

- ✓ all unsuitable sites to be reported to the E-Safety Co-coordinator immediately;
- ✓ if a safeguarding concern, report issue to S Dixon or J Elliot Immediately;
- ✓ the appropriate action will be decided by any of the above, whether to investigate, and possible disciplinary action may follow;
- ✓ all staff have a responsibility to report any concerns.

8. Managing Information Systems

All information relating to our pupils, parents and staff is confidential. You must treat all school information with the utmost care whether held on paper or electronically. The school uses the Sims MIS and the security of the system is managed by the schools network supplier RM PLC.

8.1 Local Area Networks (LAN)

- users must act reasonably – e.g. the downloading of large files, or live streaming during the working day may affect the service the other staff receive. This is measured by RM who provide reports regarding the amount and type of information downloaded;
- users must take responsibility for their network use;

- workstations should be secured against user mistakes and deliberate actions by being password protected; this is monitored via the management system and the filtering system - eSafe and Smoothwall;
- servers must be located securely and physical access be restricted;
- the server operating system must be secured and kept up to date. Microsoft server 2012 and 2016 edition.
- virus protection for the whole network must be installed and current (we do have virus protection on the server and this is checked by RM);
- access by wireless devices must be proactively managed by using RM trapeze and Meru points which are secured with a minimum of WPA2 encryption.

8.2 Wide Area Network (WAN)

The schools broadband network is protected by Smoothwall (internet filtering), the email is protected by Office 365. There is also an effective firewall protecting our school network.

- decisions on WAN security are made on a partnership basis between schools and the provider, this is controlled by RM and Dudley Metropolitan Council (DMBC);
- the security of the school information systems and users will be reviewed regularly;
- virus protection will be updated regularly by RM;
- personal data sent over the Internet or taken off site will be encrypted and password protected;
- Unencrypted portable media may not used without specific permission followed by an anti-virus/malware scan;
- unapproved software will not be allowed in work areas or attached to email;
- files held on the school's network will be regularly checked. The ICT manager will review system capacity regularly. (an RM scan takes place everyday);
- the use of user logins and passwords to access the school network will be enforced at all times this is managed by RM and the School.

8.3 How e-mail is managed

Care must be taken when using email as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. E-mail is intended to be used. For school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher.

- pupils may only use approved email accounts for school purposes, at no times will pupils receive any external emails;
- staff and pupils must immediately tell a designated member of staff if they receive offensive emails;
- the School email address will be used for communication outside of the school;

- staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team;
- Staff must not use their school email address for social media activity;
- access in school to external personal email accounts will be blocked;
- excessive social email use can interfere with learning and will be restricted;
- emails sent to external organisations should be written as per school instruction.
- the forwarding of chain mails is not permitted;
- we have a dedicated email for reporting wellbeing and pastoral issues. This is managed by dedicated staff.

8.4 How published content is managed

- the contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published;
- Karen Otton will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate;
- the school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

8.5 Publishing of pupil work or images

- images or videos that include pupils will be selected carefully and will not provide material that could be reused;
- pupils' full names will not be used anywhere on the website, particularly in association with photographs;
- written permission from parents or carers will be obtained before images/videos of pupils are electronically published;
- pupils work can only be published with permission of their parent/guardian;
- written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use;
- the School has a policy regarding the use of photographic images of children which outlines policies and procedures.

8.6 How social networking, social media and personal publishing will be managed.

- the school will control access to social media and social networking sites;
- pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc; (detailed in Pupil AUP).
- staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the

site is age appropriate. Staff will obtain documented consent from the Senior Leadership team before using Social Media tools in the classroom.

- staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are strongly advised not to run social network spaces for pupil use on a personal basis;
- personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible;
- pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private in their personnel use;
- all members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory;
- newsgroups will be blocked unless a specific use is approved (blogging/forums);
- concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites;
- staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction. Safe and professional online behaviour will be outlined in the school Acceptable Use Policy.

8.7 How filtering is managed.

Access controls fall into several overlapping types (commonly described as filtering):

- blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day, this appears as a white list and a black list of reported sites through RM networks;
- dynamic content filtering examines web page content or email for unsuitable words;
- keyword lists filter search engine searches and URLs for inappropriate results and web addresses;
- rating systems give each web page a rating for sexual, profane, violent or other unacceptable content such as radicalisation. Web browsers can be set to reject rated pages exceeding a threshold; these are the sites on the RM blacklist;
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil and staff access;

- antivirus software checks for Key loggers (record all text sent by a workstation) and analyse it for patterns;

The school will work with DMBC and the RM to ensure that filtering the policy is continually reviewed.

The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

- changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and with consent from the Senior Leadership Team;
- the School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective;
- any material that the school believes is illegal will be reported to appropriate agencies such as the West Midlands Police and DMBC child protection unit;
- the school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from RM.

8.8 Managing video conferences.

Any person wishing to use video conferencing facilities must obtain permission from a member of the Senior Management Team.

Users

- videoconferencing will be supervised appropriately for the pupils' age and ability;
- parents and carers consent must be obtained prior to children taking part in videoconferences.

8.9 Emerging technologies.

- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use & Mobile Phone Policy.

8.10 How personal data is protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the School Data Protection Policy.

8.11 Use of Star Lesson technology

Staff use Star Lesson technology as a part of their own CPD and for training purposes. Accounts are username and password protected and staff must not export video footage to an external storage device without prior permission from a member of SMT.

9. Policy

9.1 How will the Internet access be authorised?

- the school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications;
- all staff will read and sign the 'School acceptable Use Policy' before using any school ICT resources;
- parents will be prompted by 'Groupcall' and asked to read the 'Pupil Acceptable Use Policy' for pupil access and discuss it with their child, where appropriate;
- all visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy. Supply staff will be granted access to the 'supply' area of the school network only, where work for pupils is deposited by teaching staff;
- parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- when considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupils. (Angie Francis will lead this process).

9.2 How the risks are assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

- the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to West Midlands Police;
- methods to identify, assess and minimise risks will be reviewed regularly;
- regular filtering checks are undertaken as explained above;
- any unacceptable use will be investigated by the e-safety co-ordinator.

9.3 How the school responds to incidents of concern?

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc).

- the e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child Protection log;
- the Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately;
- the school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate;
- the school will inform parents/carers of any incidents of concerns as and when required.
- after any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required;
- where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the children's safeguard team or council e-Safety officer and escalate the concern to the Police;
- if the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the safeguard team or the council e-Safety Officer;
- if an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Dudley.

9.4 E–Safety complaint handling

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the head teacher. All E-Safety complaints and incidents will be recorded by the school, including any actions taken.

- parents and pupils will be informed of the complaints procedure;
- parents and pupils will need to work in partnership with the school to resolve issues;
- all members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns;
- discussions will be held with the local Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially

illegal issues;

- any issues (including sanctions) will be dealt with according to the school's disciplinary, behavior and child protection procedures;
- all members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

9.5 How is the Internet used across the community?

The school will liaise with local schools and the DMBC to establish a common approach to E-Safety.

- the school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice;
- the school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site;
- the school will provide an AUP for any guest who needs to access the school computer system or internet on site.

9.6 Cyber bullying

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyber bullying. All incidents of cyber bullying reported to the school will be recorded. There are clear procedures in place to investigate incidents or allegations of Cyber bullying.

- staff will keep a record of the bullying as evidence;
- the school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary;
- pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos;
- the bully will be asked to remove any material deemed to be inappropriate or A service provider may be contacted to remove content if the bully refuses or is unable to delete content;
- internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy;
- parent/carers of pupils will be informed;

- the Police will be contacted if a criminal offence is suspected.

9.7 How Learning Platforms are managed?

The leadership team and ICT staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities. Pupils/staff will be advised about acceptable conduct and use when using the LP. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP. When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

- any concerns about content on the LP will be recorded and dealt with following the schools procedure;
- a visitor may be invited onto the LP by a member of the leadership team. In this instance there may be an agreed focus or a limited time slot;
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfill a specific aim and may have a limited time frame.

9.8 Mobile phones and personal devices

- the use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the school mobile phone policy and the Acceptable Use Policy for staff and pupils;
- in this instance all mobile phones must be handed into pupil reception on a daily basis as per the schools mobile phone policy;
- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy;
- As per the school mobile phone policy, no phones are allowed on site during school hours and are to be handed in to pupil reception; staff will confiscate a phone or device if they believe it is being used. The pupil may be searched by a member of the senior leadership team or a pastoral manager if this is being breached;
- if there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation;
- mobile phones and personal devices will not be used during lessons or formal school time. They should be handed in at the start of the day as per the mobile phone policy';
- the Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones;

- electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual;
- mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms or toilets, this constitutes disciplinary action.

Pupils Use of Personal Devices

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

- phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations and disqualification;
- if a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school pupil reception;
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity;
- staff must not use personal mobile phones during contact time, unless by prior arrangement with the Head Teacher.
- staff will be issued with a school phone where contact with pupils or parents/carers is required;
- mobile phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances;
- if members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

- staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose;
- if a member of staff breaches the school policy then disciplinary action may be taken;
- All staff members are personally responsible for any breach of data; this will include loss of laptops. All staff should be using CC4 Anywhere/CC4 Access where sensitive data and information is concerned. No ***unencrypted*** memory sticks are to be used to store ANY personal data or data that can be deemed to hold any sensitive materials, i.e. Names, addresses, medical issues etc. If staff are deemed to have affected a breach of policy you may be personally prosecuted for this offence;
- Please keep all information secure at all times using appropriate passwords provided;
- Permission must be obtained from senior management before staff access the wireless network using personal devices; such as mobile phones and tablet pc's.

9.9 Data Protection

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorized use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of staff and the Data Manager to ensure that obsolete data are properly erased or destroyed.

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorized officer may need to disclose data without explicit consent for that occasion.

Logical Security

- no unencrypted memory sticks are to be used to store ANY personal data or data that can be deemed to hold any sensitive materials, i.e. Names, addresses, medical issues etc. If staff are deemed to have affected a breach of policy you may be personally prosecuted for this offence with disciplinary action following.

All staff are advised not to use memory sticks at all but use the schools protected area for sensitive data. All equipment that holds data must be password controlled in case a third party gets hold of the equipment. If any data or equipment with data on is lost or stolen this must be reported to the data controller as soon as possible.

It is the aim of the school that all appropriate staff are properly trained, fully informed of their obligations under the DPA 1998 and aware of their personnel liabilities.

Any employee deliberately acting outside of the recognized responsibilities may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action.

For further information please see the schools Data Protection Policy.

10.1 Pupil Awareness

Consideration will be given as to the curriculum place for teaching e–Safety. The school leadership teams' have also been involved in looking at ways to get this information across to the pupils. All users will be informed that network and Internet use will be monitored.

- pupil instruction regarding responsible and safe use will precede Internet access;
- an E-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use;
- e-Safety rules or copies of the Pupil Acceptable Use Policy will be posted in all rooms with Internet access;
- safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas;
- particular attention to E-Safety education will be given where pupils are considered tobe vulnerable.

10.2 Staff Awareness

The E-Safety Policy has been formally discussed with all members of staff. To protect all staff and pupils, the school will implement Acceptable Use Policies. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

- staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues;
- the School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils;
- all members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

10.3 Parents' Support

Parents' attention will be drawn to the school E-Safety Policy in newsletters, the school prospectus and on the school website.

- a partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings;
- parents will be requested to sign an E-Safety/Internet agreement as part of the Home School Agreement;
- parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children;
- information and guidance for parents on E-Safety will be made available to parents in a variety of formats;
- advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents;
- interested parents will be referred to organisations listed in the "e–Safety Contacts and References section";
- Parents may be asked to attend specific e-safety training if relevant.

11 Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and schools should always consult with their Safeguard Team or Safer Schools Partnership Officer from West Midlands Police if they are concerned that an offence may have been committed.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. 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). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Communications Act 2003 (section 127)

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.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing. (As per the School's Data Protection Policy).

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to: gain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber bullying/Bullying:

- Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behavior/anti-bullying policy.

All monitoring, surveillance or investigation activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-safety, However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

12 Contacts

School E-safety coordinator: Mr. Simon Carroll 6398

School SIRO: Mr Ben Stitchman 6399

Safeguarding Lead: Mr Steve Dixon or Miss Jayne Elliot 6403

Lead Governor: Mr. Tony Proctor

RM Systems controller: Mr. Inderpal Bhuller

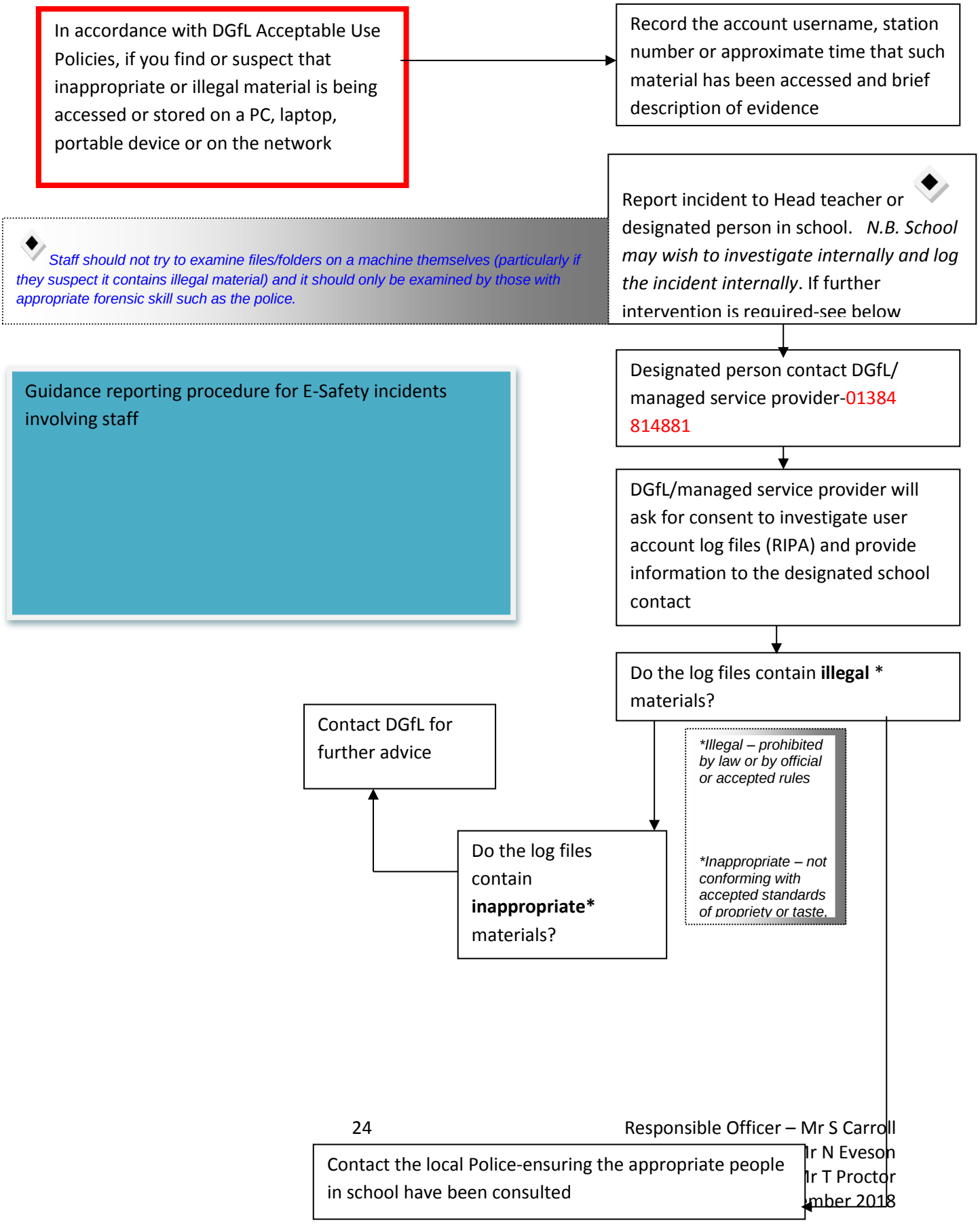
Website Controller: Mrs Karen Otton

The Dormston School E-Safety Audit:

Has the school an e-Safety Policy that complies with DMBC guidance?	
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at	
The policy is available for parents/carers to access at	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	

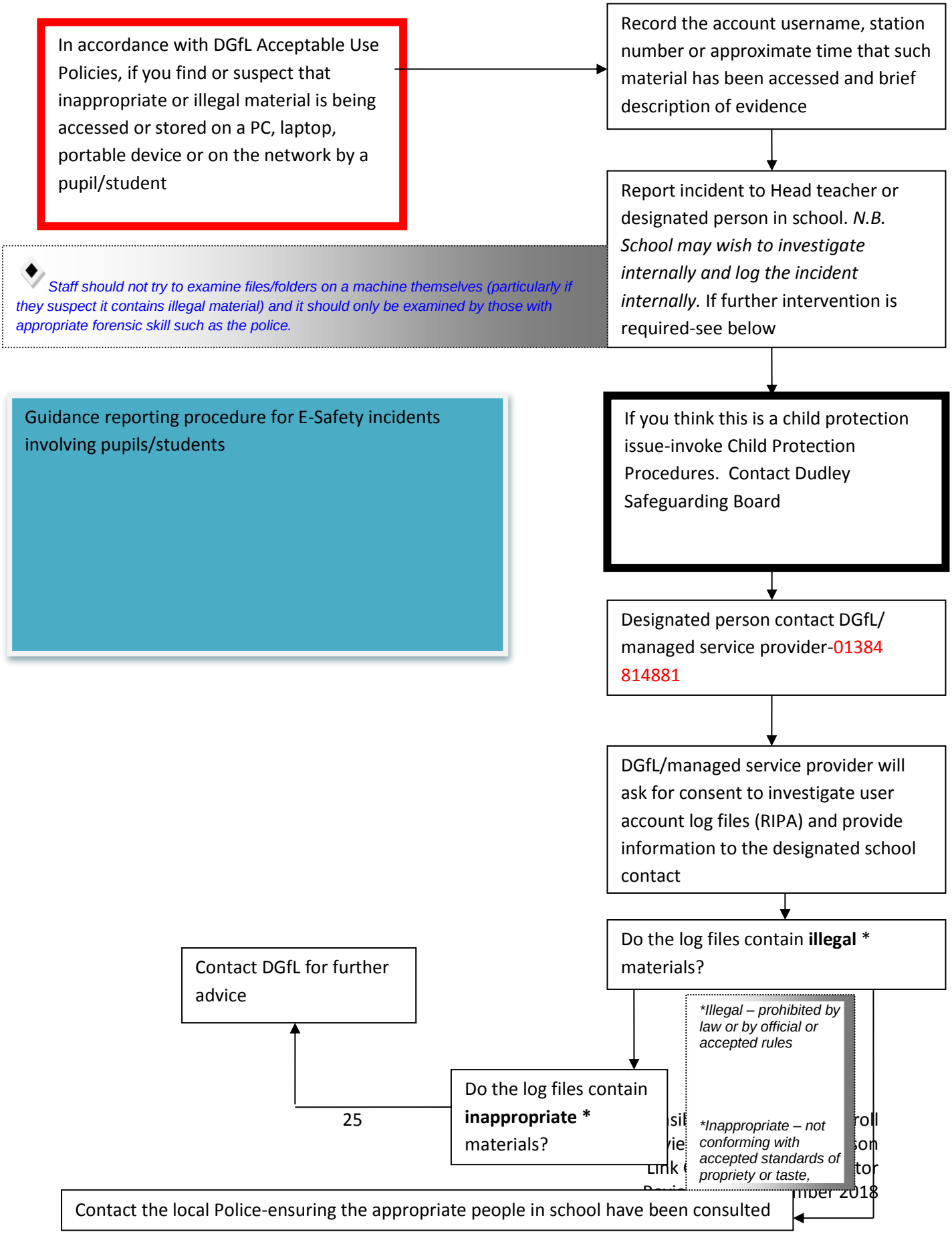
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	
Do parents/carers or pupils sign an Acceptable Use Policy?	
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	
Has an ICT security audit been initiated by SLT?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	
Does the school log and record all e-Safety incidents, including any action taken?	
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

Appendix 1- Guidance procedure for E-Safety incidents-Staff user incidents



Responsible Officer – Mr S Carroll
Mr N Eveson
Mr T Proctor
mber 2018

Appendix 1 -Guidance procedure for E-Safety incidents-Pupil user incidents



Appendix 2-E-Safety tools available on the DGfL network

E-Safety tool	Type	Availability	Where	Details
Smoothwall	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
Impero	Teacher support Filtering Workstation monitoring	Part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work. Reports inappropriate or blocked websites to class teacher.
CC4 AUP	Awareness raising	Part of CC4-needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
Email	Email communication	Provided as part of DGfL	Online through Office 365	Allows schools to restrict where email is sent from/to.