E-safety Policy and Guidance

Acceptable Use Policy for staff and pupils

DANECOURT SCHOOL

Refer to:

Behaviour policy

Child protection policy

Anti-bullying policy

Computing policy

July 2018

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

Guidance and other miscellaneous documents

Policy statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users – refers to staff, trustees, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, trustees, parents, home school worker, outreach team, auxiliary staff

Safeguarding is a serious matter; at Danecourt School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability to harm to the student or liability to the school.

This policy is available for anybody to read on our school website, upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy.

Acting Headteacher: Mr Kevin Ruddell

Chair of Trustees: David Valentine

Introduction and overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Danecourt School with respect to the use of IT-based technologies
- Safeguard and protect the children and staff
- Assist school staff working with children to work safely and responsibly with the internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use of the whole school community.
- Have clear structures to deal with online abuse such as online bullying (nothing that these need to be cross referenced with other school policies).
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

Content

- exposure to inappropriate content
- lifestyle websites promoting harmful behaviour
- hate content
- content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

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

Policy Governance (Roles and Responsibilities)

Trustees

The Trustees are accountable for ensuring that Danecourt School has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will
    1. Keep you up to date with emerging risks and threats through technology use.
    2. Receive regular updates from the senior management team/computing co-ordinator/online safety co-coordinator in regards to training, identified risks and any incidents.
    3. To approve the online safety policy and review the effectiveness of the policy.
    4. To ensure that the school has in place policies and practices to keep the children and staff safe online.

Headteacher

Reporting to the board of trustees, the Headteacher has overall responsibility for e-safety within our school. They must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant local safeguarding children board (LSCB) guidance. The day-to-day management of this will be delegated to a member of staff, the e-safety officer as indicated below.

The Headteacher will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, trustees and parents.
- The designated e-safety officer has had appropriate CPD in order to undertake the day to day duties and ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- All e-safety incidents are dealt with promptly and appropriately.
- To lead a 'safeguarding' culture, ensuring that online safety id fully integrated with whole school safeguarding.
- To ensure the school uses appropriate IT systems and services including, filtered internet services
- To be aware of procedures to be followed in the event of a serious online safety incident
- Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of the pupils, including risk of children being radicalised.
- To ensure school website includes relevant information

E-safety officer

The day-to-day duty of e-safety officer is devolved to Kevin Ruddell.

The e-safety officer will:

- Keep up to date with the latest risk to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the headteacher.
- Advise the headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail is completed.
- Ensure any technical e-safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical support.
- Make him aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the head teacher and responsible governor to decide on what reports may be appropriate for viewing.
- To ensure that all staff are aware of the procedure that need to be followed in the event of an online safety incident.
- Promote an awareness and commitment to online safety throughout the school community.
- Ensure that online safety education is embedded within the curriculum.

Computing Technical Support Staff

Technical Support Staff are responsible for ensuring that:
The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age (Note: this will require discussion as to when passwords should be changed).
- The IT system administrator password is only available to the Computer technician and Computing co-ordinator.
- That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- To keep up-to-date documentation of the school's online security and technical procedures.

Data and information (assest owners) Managers (IAOs)

- To ensure that the data they manage is accurate and up-to-date
- Ensure best practice in information management i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements
- The school must be registered with information commissioner.

All staff Users

Staff/Users/Trustees/volunteers are to ensure that

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- To read, understand and sign ad adhere to the school staff acceptable use agreement/policy, and understand any updates annually. The AUP is signed by new staff on induction.
- Any e-safety incident is reported to the e-safety officer (and an e-safety incident report is made), or in his absence to the Headteacher. If you are unsure the matter is to be raised with the e-safety officer or Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.
- To maintain an awareness of current online safety issues and guidance e.g. through CPD.
- To model safe, responsible and professional behaviours in their own use of technology.
- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or

meeting with the line manager and technician on the last day to log in and allow factory reset.

Teachers

Teachers are to ensure that:

- They embed online safety in the curriculum
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws as appropriate to their understanding.

All pupils

Teachers are to ensure that:

- Read, understand, sign and adhere to the pupil acceptable use policy annually
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- To contribute to any pupil surveys that gather information of their online experiences

The boundaries of use of computing equipment and services in this school are given in the student Acceptable Use policy; any deviation or misuse of computing equipment or services will be dealt with in accordance with the behaviour policy.

E-safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside school.

Parents and Carers

Parents should:

- Read, understand and promote the school's pupil acceptable use agreement with the child/ren.
- Consult with the school if they have any concerns about their children's use of technology
- Support the school in promoting online safety and endorse the parents' acceptable use agreement which includes the pupils' use of the internet and the school's use of photographic and video images.

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent evenings, school newsletters and the website the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules and safeguarding procedures in place to ensure that their child can be properly safeguarded. As such, parents will sign the student acceptable use policy as part of the admissions process before any access can be granted to school computing equipment or services.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions
- Online safety coordinator acts as first point of contact for any incidents
- Any suspected online risk or infringement is reported to online safety coordinator that day
- Any concern about staff misuse is always referred directly to the headteacher, unless the concern is about the headteacher in which case the complaint is referred to the chair of trustees and the LADO (local authority designated officer)

Review and monitoring

The online safety policy is referenced within other school policies (e.g. safeguarding and child protection policy, anti-bullying policy, PSHCE, computing policy)

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by the trustees. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Education and curriculum

Pupil online safety curriculum

This school:

- Has clear, progressive online safety education programme as part of the computing curriculum/PSHCE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and pupils understand issues around plagiarism, how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

Staff and trustee training

This school:

- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the online safety policy and the school's acceptable use agreements.

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

Parent awareness and training

This school:

- Provides induction for parents which includes online safety
- Runs a programme of online safety advice, guidance and training for parents.

Expected conduct and incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Technology

Danecourt School uses a range of devices including PC's, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet filtering – we use Medway Grid for learning secure private network which connects school local area networks (LAN) to the Medway Council Network. One of the services is filtering that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The computing co-ordinator, e-safety officer and IT support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. Any items that are deemed inappropriate are to be reported to MGFL support portal.

In this school:

- informs all users that Internet/email use is monitored;

- has the educational filtered secure broadband connectivity through the MGfL;
- Uses the MGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, and gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from MGfL);
- Uses DfE, LA or MGfL approved systems including 7 Zip and password protection on documents.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the MGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Email Filtering – we use Sophos anti-virus software and Malwares software that prevents any infected email to be sent from the school, or to be received by the school. Our email system is Microsoft Exchange via Medway and Atomwide which has been endorsed by Medway Local Authority. Infected is defined as: an email that contains a virus or script (i.e. Malware) that could be damaging or destructive to data; spam email such as phishing message.

This school

- Provides staff with an email account for their professional use, Staffmail email and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example office@danecourt.bptrust.org
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use Purple Mash email system.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the Microsoft Exchange systems on the school system
- Staff will use LA or Microsoft Exchange systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- If using email to transfer pupil personal data, Egress Switch is used to transfer securely.

School website

- The Headteacher, supported by the trustees, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas or the shared area or their office 365 allocated cloud space.
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB flashdrives/memory sticks) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

(Note: Encryption does not mean password protected)

Passwords – All staff will be unable to access any device without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The computing coordinator and IT support will be responsible for ensuring that passwords are changed.

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.

Anti-virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT support will be responsible for ensuring this task is carried out, and will report to the headteacher if there are any concerns. All USB peripherals such as flashdrives/memory sticks are to be scanned for viruses on a regular basis.

Safe Use

Internet – use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All users/staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. All users (office, teaching staff including teaching assistants and learning support assistants, trustees and the PTA) will be given their own e-mail address, solely for the purpose of 'business' communication.

Students will be given their own email address which will be for internal school environment only.

Digital images and video– Digital media such as photos and videos are covered in the schools 'Policy for using images of children: photographs, videos, websites and webcams (ipads and phones), and is re-iterated here for clarity. All parents must sign a photograph/video release slip as part of the admission form; non return of the permission slip will not be assumed as acceptance. This will ascertain if parents give permission for newspaper publication. **The format for both newspaper publication and website will have either just the child's first name or just their photograph and avoid using both together.**

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school and annually thereafter.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include trustees, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social Networking – there are many social networking services available; Danecourt School do not endorse or engage with parents and the wider community through social networks. Should staff wish to use other social media, permission must first be sought via the e-safety officer who will advise the Headteacher for a decision to be made. Any new service will be assessed before use is permitted.

A broadcast service, such as twitter or Facebook, is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

Staff members re strongly advised that being 'friends' with other staff is high risk. Staff members that are also parents are very strongly advised not to be 'friends' with parents and staff.

In addition, the following is to be strictly adhered to:

- Permission slips (via school photography policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated"

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use.

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact for key school information (data controller - headteacher) is. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

- We use the LGfL USO Auto Update, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- All mobile devices will be handed in at reception should they be brought into school.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is prohibited. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras are not permitted for use in school.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.

If a member of staff breaches the school policy then disciplinary action may be taken.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Notice and a down policy – should it come to the schools attention that there is a resource which has inadvertently uploaded, and the school does not have the copyright permission to use that resource, it will be removed within one working day.

Incident Management – any e-safety incident is to be brought to the immediate attention of the e-safety officer, or in his/her absence the Headteacher. The e-safety officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, MGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Training and curriculum – it is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Danecourt School will have a programme of training which is suitable to the audience.

E-safety for students is embedded into the curriculum; whenever computing is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. This will take place over the whole academic year using the computing curriculum that is suitable for the new National Curriculum 2014.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents. Safer Internet Day will be highlighted s part of an assembly and posters will be placed around the school.

The e-safety officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Trustee for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the headteacher for further CPD.

The e-safety training programme has been established as part of the school improvement plan.

Why we filter the internet

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an internet filter there are two important aspects:

Very broadly speaking

- Filtering – this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- Monitoring – this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for internet misuse.

These terms are important; mention to anyone that you are monitoring their internet use and the immediate vision is of somebody sat at a computer screen watching every move and click; that is simply not the case.

The fact that an internet filter is in place to filter and monitor activity is of particular importance because you then have questions raised of morality such as, "It's my human right to privacy". "big brother is watching", and others.

Consider CCTV at school; everybody knows it is there because you can see it and there are signs telling people that they are being monitored. Everybody knows why it is there whether they agree with it or not… it is justified for the protection and safety of children and staff whilst in school, and also the protection of the building and its contents.

But what about internet filtering? How many of the parents know that the online activity of their child may be monitored? How many of the staff know? Importantly, do they know why? Whilst the answer should be 'yes' to all, this is not the case and normally with good reason; how do you know what you don't know?

As with many things we do in life it is all about managing expectations, commonly known as justifying ourselves. But it is that justification that gives us precedence for doing something that others may deem controversial.

Why do we Filter and monitor?

Danecourt School filter internet activity for two reasons:

We filter to ensure

- (As much as possible) that children and adults are not exposed to illegal or inappropriate websites. These sites are restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (As much as possible) that the school has mitigated any risk to the children and adults, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and adults.

We monitor for assurance

- (As much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

It is the expectation of the user that is particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however you are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that you are monitoring them. By making reasonable efforts you are working 'with' the students and parents, not just merely telling them.

In reality, very few schools actually monitor internet activity, and neither do local authorities (remember, monitor is different to filter). Whether that is right or not is out of scope for this paper, but the fact is you could, in fact Ofsted make clear that schools should be managing their own filter, and this would include monitoring for inappropriate activity, overly-restrictive filtering or otherwise.

Of course, some will disagree with what you are doing, but that is their right and again consent is not a requirement. It is the understanding, not the consent which is important.

Summary

- Filtering is different to monitoring
- You do not require consent
- Tell users if you do monitor, or you have the facility to monitor
- Set user expectations; explain under what circumstances it may be a requirement to monitor
- Ensure that users are informed that internet use 'may be subject to monitoring' in the acceptable use policy.
- Ensure parents are informed, the reason why monitoring may take place, and the parent acceptable use form is signed and understood.

E-safety Incident log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Trustee)		Date:	

Risk Assessment (Example)

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and wellbeing of the child.
Likelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using Sophos software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Policy: How will infringements be handled?

Whenever a pupil or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as <u>exemplification</u> only:

PUPIL	
Category A infringements	Possible Sanctions:
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	Refer to class teacher Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	Possible Sanctions:
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, Newsgroups • Use of File sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc. • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Refer to Class teacher/ Head of Department / Online-Safety Coordinator Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]
PUPIL	
Category C infringements	Possible Sanctions:
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material	Refer to Class teacher /Online-Safety Coordinator / Head teacher / removal of Internet access rights for a period Escalate to: contact with parents / removal of equipment Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

Category D infringements	Possible Sanctions:
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	Refer to Head Teacher / Contact with parents Other possible safeguarding actions: • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).

STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	Referred to line manager / Head teacher Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	Possible Sanctions:
• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	Referred to Head teacher / Governors; Other safeguarding actions: ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. ▪ Identify the precise details of the material. *Escalate to:* *Report to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.

DANECOURT SCHOOL	Name of School	Danecourt
	Policy review Date	June 2018
	Date of next Review	June 2019

Written by Kevin Ruddell (based on Alan Mackenzie's e-safety policy www.esafety-advisor.com and lgfl policy).