New Earswick Primary School

"To have the best, to do our best, to be the best that we can be."

E Safety Policy

Written: September 2022
Review due: September 2023
Governance review: HT

CONTENTS

This policy has been adopted by the Board of Directors of the Pathfinder Multi Academy Trust and is applicable across all schools that make up the Pathfinder Multi Academy Trust. In line with the MAT's Scheme of Delegation, this Policy must be duly applied by each Local Governing Committee and the Head Teacher of each school that is part of the Pathfinder Multi Academy Trust.

Where there are specific details or any discretions in the policy that apply to an individual school or Local Governing Committee this has been made clear within the wording of the policy.

This policy will be monitored regularly by the MAT Head Teachers Group and reviewed formally by the Pathfinder MAT Board of Directors in line with the agreed timetable for policy review or sooner as events or legislation changes require.

DATE ADOPTED: September 2022

DATE FOR REVIEW: September 2023

.

E-Safety Policy

Contents

1. Introduction and Overview

Rationale

- Set out the key principles expected of all members of the school community at New Earswick Primary School with respect to the use of COMPUTING-based technologies.
- Safeguard and protect the children and staff of New Earswick Primary School and comply with GDPR (General Data Protection Regulation).
- Assist school staff working with children to work safely and responsibly with the internet and other 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.
- Have clear structures to deal with online abuse such as cyberbullying which are 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.

Areas of Risk for our school community:

- ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- exposure to inappropriate content, including online pornography,
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- Data breach
- hate sites, sites inciting radicalisation and/or extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Messaging

ROLES

Role	Responsibility
Head teacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security GDPR compliant • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious eSafety incident. • To receive regular monitoring reports about E-Safety from Computing Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures Review and monitor: • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Computing Lead and DSL	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with school COMPUTING technical staff • To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • To ensure that an e-Safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data
Governors	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub committee • To support the school in encouraging parents and the wider community to become engaged in e-safety activities
Computing lead	• To oversee the delivery of the e-safety element of the Computing curriculum • To address e-safety issues as they arise promptly • To promote E Safety news and advice with the community
Outside Technical	• To report any e-Safety related issues that arises, to the Computing Coordinator.

support (VITAL)	• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school Computing system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that the use of the *network / remote access / email/School Twitter account* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator/Data Protection Lead /Head of School for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
GDPR Manager	• To take overall responsibility for data and data security • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • Report breeches as set out by GDPR MAT guidance
Teachers	• 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 • To follow and adhere to the Staff Protocol booklet.
All Staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety coordinator To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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 know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's ESafety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies
Parents	• To support the school in promoting e-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 • To engage with documentation shared by the school. • To adapt to the online rules during home learning to promote safe on line learning.

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

- Policy to be posted on the school website/ staffroom.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- 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. Neither the school nor PMAT can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview/counselling by teacher / Phase Leader / e-Safety Coordinator / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
    - referral to LA / Police.

- Our Head teacher acts as first point of contact for any e-safety complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

2. Education and Curriculum

Pupil e-Safety curriculum

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHCE curriculum. It is built on LA / LGfL e-Safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to think before you click on a website or share information
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - E-Safety Ambassadors are appointed from Years 4, 5 and 6; ○ to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post photos or videos of others without their permission;
    - to know not to download any files – such as music files - without permission; ○ to have strategies for dealing with receipt of inappropriate materials; ○ [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

The curriculum will:

- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in popups; buying on-line; on-line gaming / gambling;

Parent awareness and training

We run a rolling programme of advice, guidance and training for parents to ensure that principles of e-safety behaviour are made clear, including:

- Information leaflets;
  - in school newsletters;
  - on the school web site;
  - demonstrations, workshops, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Student / Pupil Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

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

The school will try to ensure that pupils have good access to ICT to enhance their learning. The school will, in return, expect pupils to agree to be responsible users.

Acceptable Use Policy Agreement

Staff are responsible for reading the school's e-safety policy and using the school COMPUTING systems accordingly, including the use of mobile phones, and hand held devices. Staff are responsible for pupil data safety so that it is GDPR compliant

Parent recordings

The school does not permit parents/carers to take photographs and videos of any other child/children at school events however at the end of assembly parents/carers are permitted to take photos **of their own child/children only** and that the school requests that photos/videos are not shared on any social networking site such as Facebook, WhatsApp, snapchat, twitter etc. (However, this matter is subject to discussion and approval at the Parents' Forum annually.)

STAFF CODE OF CONDUCT

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, emails and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it with anyone, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on–line.
- I will not arrange to meet people I have met only online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

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

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

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use a mobile phone in school.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites on school equipment.

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

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement. This applies both in school, and when I am out of school where it involves my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable User Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signed: _____ Date: _____

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student / Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Policy, to which it is attached. It is simplified to age-appropriate child- friendly language. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Using the computer

- ✓ I know that my teacher will check what I am doing
- ✓ I will keep my passwords safe and won't share them with anyone 'like my tooth brush!'
- ✓ I will be aware of stranger danger online
- ✓ I will not share my name, address or other details with anyone online
- ✓ I will not arrange to meet anyone
- ✓ I will tell an adult if I spot something that make me uncomfortable
- ✓ I will use RESPECT online to everyone
- ✓ I will not upload or download without permission
- ✓ I will not use social media for older people
- ✓ I know that I am breaking school rules if I do any of these.

I have read and understand the above and agree to follow these guidelines when:

- ☐ I use the school ICT systems and equipment (both in and out of school)
- ☐ I use my own equipment out of school in a way that is related to me being a member of this school e.g. accessing school email, website etc or communicating with other members of the school.

Name of Student / Pupil

Class

Signed _____ Date _____

Applicable for those able to agree subject to age. I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community 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 (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /PMAT
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Data breaches are reported to our Data Protection Lead (DPL) is **Mrs Oswald** and **Mr Fletcher**. Our Data Protection Officer (DPO)

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords to enter our MIS systems
- We require staff to change their passwords into the MIS, LGfL USO admin site, Every 90 days.

Email Policy

- All staff to adhere to school's Email protocol and email use policy
- Provides staff with an email account for their professional use, *pmat*
- 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.

- Any apps educational (Espresson, Digimaps etc) and /or Classroom management (Class Dojo) used by school are GDPR compliant.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Any personal or business use for illegal, threatening, offensive, obscene, pornographic or libellous purposes by staff is strictly prohibited.
- Knows that spam, phishing and virus attachments can make e mails dangerous
- Access in school to external personal e mail accounts is not permitted and may be blocked
- Never use personal email to transfer staff or pupil personal data. We use secure lGfl e-mail account.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted; ○ embedding adverts is not allowed;
- All staff sign our school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
- A letter sent to anyone using the school letterhead must be approved by the head teacher.
- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school events on personal social networking sites such as Facebook. Twitter etc
- Staff must not use social networking sites within lesson times
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy

Video Conferencing

This school

1. Only uses Teams and Zoom supported services for video conferencing activity;
2. Only uses school iPads, chrome books or school owned devices to access these

CCTV

○ We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*),

without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer (Also check our Data Protection Policy, Data Retention Policy and safeguarding policy)

Personal mobile phones and mobile devices

- Mobile phones 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.
- Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils during the 'Wake Shake Up' routine or at other times in the school playground.
- Student mobile phones, MP3 players, iPads, smart watches which are brought into school must be turned off (not placed on silent) and handed in to the class teacher on arrival at school/ handed into the school office to be locked away.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone they may seek specific permissions to use their phone at other than their break times.
- Staff mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned 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 phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar 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.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the head teacher.
- Images and content recorded for twitter updates will be deleted from the school equipment once it is posted.

Use of digital images

- 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;
- 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;
- 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 use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Photos/videos taken on school iPads are stored on the school network.
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, 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 identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Incidents and possible outcomes

Incidents	Refer to class teacher	Refer to a senior member of staff	Refer to Police	Refer to technical support staff for action re filtering /security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. loss of minutes Isolation/ detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓	✓		✓	✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓		✓	✓		✓	✓
Unauthorised use of social networking / instant messaging / personal email	✓	✓		✓	✓		✓	✓
Unauthorised downloading or uploading of files	✓	✓		✓	✓		✓	✓
Allowing others to access school network by sharing username and passwords	✓	✓		✓	✓		✓	
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓		✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings of sanctions	✓	✓	✓	✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓		✓	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓	✓	✓		✓

Accidentally accessing offensive or pornographic material and failing to report the incident							✓	

0

Deliberately accessing or trying to access offensive or pornographic material	✓		✓	✓	✓	✓		✓
Receipt of transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓	✓	✓	✓		✓