East Midlands Education Trust

Online-Safety Policy

Spring 2023

Review Date:	Spring 2023	Reviewed & adopted by:	Trustees
Next Review Due:	Spring 2026	Updated by:	Trust Safeguarding Lead
Mid-Reviews *(statutory):*			
Document No:	POL-SCH-006	*The information contained on this document is considered proprietary to East Midlands Education Trust in that these items and processes were developed at private expense. This information shall not be released, disclosed, or duplicated.*	

Contents

1 Context 3

2 The technologies involved 4

3 Whole school approach to the safe use of ICT 5

4 Roles and Responsibilities 5

5 Social Media and e-Safety 6

6 How will complaints regarding e-Safety be handled? 7

Appendix 1 - Websites for parents and carers 8

Appendix 2 - Student Guidelines for Acceptable Use of ICT (Version 3.0 Sept 2015) 10

Appendix 3 - Staff Computer Use Guidelines 12

Appendix 4 – Staff Laptop/Tablet/Smartphone Loan Agreement 14

Appendix 4A - Covid-19 Student Laptop Loan Agreement ..... **Error! Bookmark not defined.**

Appendix 5 - Student Information Protocol 16

Appendix 6 - Key Information for Parents 17

Appendix 7 - Technical Systems to support e-Safety 18

1 Context

1.1 The *'Online Safety in Education' Report',* published December 2015, set out the UKCCIS (UK Council for Child Internet Safety – a body set up by government to share best practise between government, charities, academia, and industry) guidance on good practise for taking a strategic approach to the future development of ICT safety education in the UK.

> "*The internet has an essential role to play in children's education, but it can also bring risks, which is why we must do everything we can to help children stay safe online – at school and at home. This includes ensuring young people know how to use the internet responsibly and that parents and teachers have the right measures in place to keep children safe from exploitation or radicalisation. We must provide helpful support and information for professionals and parents so we are all equipped to help protect children in this digital age."*

The UK Council for Internet Safety (UKCIS) is the successor to the UKCCIS, with an expanded scope to improve online safety for everyone in the UK. Our schools follow UKCIS guidance to keep children and young people safe online. This is reflected in the EMET Safeguarding and Child protection policy.

1.2 Keeping Children Safe in Education (2022) sets out how schools, organisations and individuals should work together to safeguard and promote the welfare of children. Specific online safety content has been added and strengthened in part Two to ensure online safety is viewed as part of a school's statutory safeguarding responsibilities. Part Two signposts DSLs and school leaders to the DfE 'Harmful online challenges and online Hoaxes' guidance published February 2021

1.3 Safeguarding and promoting the welfare of children includes::

- protecting children from maltreatment, neglect, violence and sexual exploitation
- Preventing the impairment of children's mental and physical health or development
- Keeping children safe from accidental injury and death
- Protecting children from bullying and discrimination
- Keeping children safe from crime and anti-social behaviour in and out of school
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- Protecting children from radicalisation
- Taking action to enable all children to have the best outcomes

1.4 Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. Other dangers include:

- Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of / sharing of personal information
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.5 Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). It is impossible to eliminate risks completely. It is essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they can face them with the skills and confidence to deal with them.

1.6 It is the duty of our schools to ensure that every child in our care is safe, and the identical principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1.7 This policy document is drawn up to protect all parties – the students, the staff and schools and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1.8 Following school responses to the Covid pandemic, there has been an increased use of technology as a tool to facilitate children and young people's learning. KCSIE 2022 continues to strengthen the important message of online safety being recognised by all schools and colleges as a key, safeguarding consideration and provides important information and guidance to ensure that all school leaders take the necessary steps to protect their communities online.

2 The technologies involved

2.1 ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children may include:

- The Internet
- e-mail
- Instant messaging providers often using simple webcams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular: Twitter, Instagram, Facebook, Snapchat, tiktok)
- Video broadcasting sites (Popular: YouTube)
- Chat Rooms (Popular: Teenchat)
- Gaming Sites (Popular: Miniclip, Minecraft
- Music download and streaming sites (Popular: Apple iTunes, Spotify)
- Mobile phones with camera and video functionality

- Smart phones with e-mail, web functionality, instant access to social networks and video conferencing).
- Other technical devices with internet capabilities

3 Whole school approach to the safe use of ICT

3.1 Creating a safe ICT learning environment includes five main elements at our schools:

3.1.1 An effective range of technological tools including;
- An industry standard internet filter on all email and internet use. The filter will maintain an up-to-date live database blocking material including; pornography; inappropriate imagery; radicalization; social media and criminal behaviour;
- Clearly flagged auditing of staff and student ICT use while in school;

3.1.2 Policies and procedures, with clear roles and responsibilities;

3.1.3 A shared understanding of safe and responsible use of ICT, the internet and devices. For secondary, the signing of a school Acceptable Use Policy by students (an example of which is in Appendix 2), and education as to why such a document is necessary.

3.1.4 Controls around the use of mobile phones and devices in school.
Students can bring mobile phones to school from the point where a student has parental permission to walk home alone. The school will set out procedures for collection and secure storage of phones during the day and return on leaving. Thereby preventing the dissemination of unfiltered content while at school.

3.1.5 A comprehensive Online Safety education programme for students, staff and parents
- Students: via the core ICT curriculum, tutorial activities, PSHE and Assembly;
- Staff: via Staff Induction and the Staff Handbook;
- Parents: via the website, Parent communication platform & Parent Handbook.

4 Roles and Responsibilities

4.1 Online Safety is recognised as an essential aspect of strategic leadership in each school and the **Principal/Head Teacher** aims to embed safe practices into the culture of the school. The Principal/Head Teacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for online Safety has been designated to a member of the Leadership team.

4.2 Each **e-Safety Coordinator** ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP)[5]. Each school's e-Safety Coordinator ensures all appropriate bodies are updated as necessary.

4.3 We ensure our **Governors** are aware of our local and national guidance on e-Safety.

4.3.1 All governors and trustees should receive appropriate online safety information/training as part of their Safeguarding and child protection training. This will form part of new governor/trustee induction and will be regularly updated.

4.3.2 Governors and trustees will ensure that school leaders and relevant staff have an awareness and understanding of the school's filtering and monitoring systems, manage them effectively and know how to escalate concerns when identified.

4.4 All **teachers** are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

4.5 All **staff** should be familiar with the policy including:

- Safe use of e-mail;
- Safe use of the Internet including use of internet-based communication services, such as instant messaging and social networks;
- Safe use of the school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Guidance on the publication of pupil information/photographs and use of websites;
- Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

4.6 Staff are reminded /updated about e-Safety matters via the Staff Handbook at least once a year.

4.7 Parents will receive regular communications from schools to reinforce the importance of children and young people being kept safe online.

5 Social Media and e-Safety

5.1 The use of Social Media at home often intrudes on school life. While an extraordinary resource it can also be used in ways that act contrary to spirit and message of the 'Keeping Children Safe in Education 2022 document.

5.2 The Education and Inspections Act 2006 empowers head teachers/principals, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The majority of these issues are linked to Social Media use.

5.3 Schools expect that students will continue to show respect to other members of the school community when off site. To clarify this point:

- Students should not bully, intimidate, abuse, harass or threaten other members of the school community.
- Students should not install, uninstall, download, upload or in any way alter school software.
- Students should not post content that is hateful, threatening, pornographic or incites violence against others.
- Students should not impersonate or falsely represents other members of the school community.
- Students are expected to show respect to the good reputation of the school and its staff.
- Students should not film, record or photograph members of the school community without their express permission, and that of the school.

5.4 The school behaviour policy states that devices can be seized, searched and deleted if the school believes the images or recordings could be used to do harm.
Searching Screening Confiscation Guidance July 2022

6 How will complaints regarding online Safety be handled?

6.1 All schools take all reasonable precautions to ensure online 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. Schools therefore cannot accept liability for material accessed, or any consequences of Internet access.

6.2 Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview / counselling by tutor / those with pastoral responsibility / e-Safety Coordinator or a member of senior staff;
- 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 the external support services.

6.3 Our e-Safety Coordinators act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal/Head Teacher.

6.4 Complaints of cyberbullying are dealt with in accordance with a school's Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school's Safeguarding and Child Protection procedures.

Appendix 1 - Websites for parents and carers

AbilityNet
AbilityNet helps disabled adults and children use computers and the internet by adapting their computer equipment.
https://abilitynet.org.uk/

Anti-Defamation League
The Anti-Defamation League helps fight anti-Semitism, extremism and hatred. They have a free filter that you can download called the 'hate filter' which protects children from known hate sites. They also have a section called 'A Parent's Guide to Hate on the Internet'.
https://www.adl.org/

ChildNet International
This website can be used for teenagers. It focuses specifically on the risks in all interactive services where young people can meet with other people, including chat rooms, mobile phones and online games. It has lots of case studies and good advice.
http://www.childnet.com/young-people/secondary

Child Exploitation and Online Protection Centre
The child exploitation and Online Protection (CEOP) Centre works across the UK and maximises international links to deliver a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities.
http://www.ceop.gov.uk/

Childnet's Kidsmart
Kidsmart has a parents' section with a range of advice and resources. There are several versions of the parents' 'KnowITAll' section which can be watched and listened to as well as fact sheets on specific issues like spam.
https://www.childnet.com/resources/looking-for-kidsmart/

Cyber Choices Programme
This is a national programme, co-ordinated by the National Crime Agency to help people make informed choices and use their cyber skills in a legal way.
https://www.eastmidlandscybersecure.co.uk/cyber-choices

NHS
For more information on how to protect your child from cyberbullying see the following website run by the NHS:
http://www.nhs.uk/Livewell/Bullying/Pages/Cyberbullying.aspx

GetSafeOnline
GetSafeOnline is a new website which focuses on online security and protection issues. It contains advice about firewalls, spyware and antivirus protection as well as how to protect your child.
Get Safe Online | The UK's leading Online Safety Advice Resource

Kidscape
For parents, guardians or concerned relatives and friends of bullied children, the charity Kidscape offer a hotline for advice with trained for counsellors. The Helpline is available on 08451 205 204 Monday-Friday from 10.00am-4.00pm.
www.kidscape.org.uk

Think U Know
This website is created by the Child Exploitation and Online Protection (CEOP) Centre and contains loads of information on how to stay safe online. All hot topics are covered – including mobiles, blogging and gaming sites.
http://www.thinkuknow.co.uk/

UKCIS
The UK's Council for Internet Safety (UKCIS) – formed by Government as a collaborative body sharing expertise from a range of organisations in the tech industry, civil society and public sector. Their sole aim is to ensure safer use of the internet, particularly for children and young adults and to make the UK the safest place to be online.
UK Council for Internet Safety - GOV.UK (www.gov.uk)

TECHNICAL SOLUTIONS

Ad-Aware Spyware is designed to go unnoticed. Lavasoft's Ad-Aware is a program you can download to look for spyware and adware on your computer and delete it.
Adaware: The Best FREE Antivirus & ad block

Firewalls
Another way to stop advertising services like pop-ups is to install a firewall. Products such as AVG will let you know when software on your system is trying to send data out to the internet and block it. Although this may sound like an extreme solution for your home PC, a firewall is arguably the best ongoing protection against this kind of invasion of privacy. You can download AVG for free from the internet.
www.avg.com

Windows 10 based PC's come pre-loaded with Windows Defender.
http://windows.microsoft.com/en-gb/windows-10/getstarted-protect-your-pc

Appendix 2 - Student Guidelines for Acceptable Use of ICT (Version 3.0 Sept 2015)

Mornington Primary School

ICT AUP (Acceptable Use Policy)

Mornington Primary School provides ICT resources for students to use, including PC's, laptops, specialist software, access to the internet, a virtual learning environment, shared group resources and printing. This continues to bring huge diversity to our curriculum. ICT resources are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these responsibly and help to ensure they remain available to all.

Equipment and School Network

- Do NOT: install, uninstall, download, upload or alter any school software
- There is no need for a memory stick and access to them is prohibited
- Damaging, disabling, harming the operation of computers or intentionally wasting resources is NOT permitted
- Computers and all associated hardware, cables, keyboards, mice, monitors, printers etc. should be left in full working order (as you found them) and any malfunctions reported to the teacher immediately
- Protect computers from spillages /damage / germs / dirt by NOT: eating, drinking or chewing gum in ICT rooms

Security and Privacy

- Protect yourself by keeping your password confidential; never use someone else's login name or password
- Other computer users should be respected and should not be harassed, harmed, offended or insulted
- Once a student has logged in to a computer, only that student should be using it
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass, alter or in any way access areas of the system which are restricted, is NOT permitted
- If you suspect your account security has been compromised in any way, you should report it to your teacher immediately. Knowingly allowing others to use your account for whatever purpose is NOT permitted
- Accessing someone else's account for whatever reason is NOT permitted

Online

- You should only access the Internet in school for authorised & supervised activities, using the school software
- Your teacher will ALWAYS supply guidance on the type of websites to use…see the next point
- These activities could be interpreted as being off task: gaming, surveys, quizzes, social networking, buying, selling, financial transactions, external emails, music, TV, movies,

news, sport, weather, maps, street view, videos, images, animations, jokes, travel, fashion, shopping, products, celebrity, gossip, external club websites, newspapers, wiki's, blogs, chat, forums, tickets, shows, events, concerts, timetables, prices, venues, holidays

- Only access suitable material: Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive or deemed in any way inappropriate is NOT permitted
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws

School Email

- Be polite and appropriate in all email exchanges
- Only use the school e-mail system for school purposes
- Do not use or access your own private email accounts in school
- Do not access email attachments that have been sent from outside school

Monitoring

- Every key you type / program you run is recorded and logged (down to left and right mouse clicks). These logs can be retrieved and have been used in evidence when someone has not followed the rules in this policy
- Your computers and screens can be continually monitored and recorded by your teachers, senior members of staff and the technicians from anywhere in the school. Random checks are made. Evidence gathered this way has been used when someone has not followed the rules in this policy

Confirmation you have read and fully understood this entire ICT AUP (Acceptable Use Policy)

Access to ICT facilities is a privilege, NOT a right. Breaking the rules of this AUP may lead to action as per the school's behaviour policy. For serious violations of this AUP: extended online bans, isolation or exclusion may be imposed.

I have read and fully understand this AUP and agree to follow its rules:

Student Name : _____

Signature: _____

Date: _____

EXAMPLE

Mornington Primary School

Computer Guidelines / Access and Passwords

It is important to remember that the School data and the systems within which it is held is a valuable asset and we must all help to protect this. It becomes expensive if we have to re-generate the data and the costs – financially and in terms of reputation - if data falls into the wrong hands or is simply lost, can be extensive.

If allocated passwords for using computer systems do not share these with others at any time unless they are a shared password and you are informed of this.

When choosing a password choose a password that will be secure and not easily identifiable. The school password protocol is; 8 letters, a mix of upper and lowercase characters and a minimum of one numeric character.

The School will provide school based computer facilities for authorized users to use as part of and in the course of undertaking their job. Access to all systems is granted with the understanding that the user accepts responsibility for the following conditions.

1. It must only be used in the execution of tasks on behalf of the School. The facility is not provided for personal usage.
2. Any downloading of, or publication on the internet of offensive material is a disciplinary offence which could lead to dismissal.
3. Publication or the electronic transference of any material that could be regarded as derogatory, relating to the School, its operations, its staff or its pupils is a disciplinary offence, which could lead to dismissal.
4. All reasonable precautions must be taken to avoid virus infection of the School's computer system. Deliberate downloading of viruses is a disciplinary offence. Any virus detected must be reported to the School ICT team immediately.
5. Personal data on staff and students e.g. home address, contact details, medical or family information should not be retained on laptops.
6. Professional and personal etiquette are a central part of our way of working. A mutual respect between colleagues is as vital in electronic communications as it is in face to face conversations and must be maintained at all times.

School maintain an audit trail of internet activity and may use this as evidence of misuse of the facility, or breach of the above conditions of use.

Computers in school should be configured for Microsoft Outlook or suitable equivalent to manage the email account of the primary user. This can be done by the user (using help sheet) or by ICT technician. If staff take laptops home, they will be able to access their Mornington Primary email accounts. Staff may **choose** to configure their home PCs to access their Mornington Primary email accounts or alternatively they can sign on to access emails over the Internet.

Staff should check emails at least once each day – ideally as often as they would check pigeon holes. Many staff – e.g. Senior Management, Pastoral Heads and Pastoral Assistants - would expect to check emails much more often.

Teachers' laptops need to be configured so that alerts with the email content **do not appear** on screen – this could be embarrassing when projecting onto a white board during a lesson.

Teachers may receive messages requiring urgent attention in a lesson. They should use their professional judgement as to whether it is necessary to reply during the lesson, bearing in mind that Teaching and learning is the priority in the lesson. In addition, the content of messages received or sent should **never**, under any circumstances, be displayed to students – "Freezing" the whiteboard display could enable urgent messages to be read and replied to.

Staff should exercise the same professional standards when using email to communicate with parents as they would when communicating by telephone or letter. Parents will be encouraged to make initial contact through the office email address. On occasions the teachers may feel it is in the best interest of the student to email parents directly. It is good practice for teachers to copy email messages to parents to relevant SLT members.

The school will not publish teachers' email addresses to parents, but clearly once a teacher replies, their address is "open" for further direct communication. Teachers should refer to senior staff any messages they are unhappy about.

The content of emails should meet professional standards. Comments made in email will be treated in the same way as written comments. Staff should also be aware of the Freedom of Information Act in that any written communication/information held about a student or a member of staff may have to be provided on request (and that this does include emails).

School Dojo App

The Dojo App allows the Instant Messaging of parents via their notification screen. Where this facility is used messages should conform to the school's standards of professionalism.

Appendix 4 – Staff Laptop/Tablet/Smartphone Loan Agreement

EXAMPLE

Mornington Primary School

We believe that a laptop, for the purposes of teaching and learning, is a 'tool of the trade'. Subsequently we aim to provide all teaching staff with a laptop. In some instances, staff are issued with a tablet depending upon the nature of the work they undertake and the environment in which they operate. However, all equipment is issued under the terms and conditions of this agreement.

1. The 'equipment' remains the property of the school at all times.
2. The 'equipment' is intended for the execution of tasks on behalf of the school. The manner by which it is used should not, in any way, impair this primary function.
3. When leaving the employment of the school all staff are required to hand back this 'equipment' to our ICT technicians on their last working day in school. A failure to return the 'equipment' will result in a salary stoppage to the value of the replacement of the item.
4. The 'equipment' must be returned to the school in the event of a long term absence either through illness, maternity leave or such like and made available for use by others. Long term absence would be deemed as being 20 days.
5. Any downloading of, or publication on, the internet of offensive material through the use of this 'equipment' is a disciplinary offence which could lead to dismissal.
6. Publication or the electronic transference of any material that could be regarded as derogatory, relating to the School, its operations, its staff or its pupils using this 'equipment' is a disciplinary offence, which could lead to dismissal.
7. All reasonable precautions must be taken to avoid virus infection of the School's computer system. Deliberate downloading of viruses is a disciplinary offence. Any virus detected must be reported to the School ICT team immediately.
8. All reasonable precautions must be taken to avoid the loss of confidential data relating to staff, parents and children which may be contained on the 'equipment'.
9. Professional and personal etiquette are a central part of our way of working. A mutual respect between colleagues is as vital in electronic communications as it is in face to face conversations and must be maintained at all times.
10. The 'equipment' must be kept secure at all times, especially when travelling. Passwords must be used to secure access to data to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.
11. With wi-fi enabled equipment you must be particularly vigilant about its use outside the school and take any precautions required by the IT support team from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

12. Should the 'equipment' be lost, stolen or damaged through negligence on the part of the member of staff the school may require the member of staff to pay for its replacement. The levels of negligence determined by the school's insurers will be used in this judgment.

I agree to observe all the conditions in the above agreement and will observe them at all times. I understand that violation of these rules could result in disciplinary action which could involve sanctions up to and including dismissal.

Name…… (please print name)

Signed……. Date……...

Appendix 5 - Student Information Protocol

<table>
<tr><td>Rationale:</td><td colspan="3">The School holds an increasing amount of data about students. The information is stored in ways that allow it to be far more portable, copiable and transmittable. Respect for our students and their privacy – as well as that of their families – would mean that we would take the utmost care of such information. This expectation has been heightened by recent failures in data security within several public bodies and considerable publicity focusing on identity fraud – with a consequent increase in public awareness around this issue. It is in this context that the DCSF has set targets for ‘real-time, online reporting’ to be accessible to parents and that the School has decided to develop its own response to this direction.</td></tr>
<tr><td>Definition:</td><td colspan="3">Student Personal Information includes:</td></tr>
<tr><td></td><td>UPN Name Contact Details: Address, Phone and Email Parent and other family details</td><td>Ethnicity Achievement Data SEN status Targets & Predictors</td><td>Progress Reports Behaviour Events GT Status</td></tr>
<tr><td>Guidelines:</td><td colspan="3">If possible – within the requirements of the work we have to do - Student Personal Information (as defined above) should not be removed from the School site in either a physical form or digital form.</td></tr>
<tr><td colspan="4">If removed in a physical form e.g. A card folder containing paper, then the utmost care should be taken. This includes placing them out of sight when travelling in a car, on a train or bus.</td></tr>
<tr><td colspan="4">Our commitment to data privacy means that only those should see the data…should see the data! Should you let your 12-year old daughter add up the marks of the year 11 mock exams… no.</td></tr>
<tr><td colspan="4">If data is removed via digital media – a laptop, portable hard-drive, flash stick, DVD or CD – then files containing personal information should be – at the very least – be password-protected and if practical, encrypted.</td></tr>
<tr><td colspan="4">If – as is preferable – the data never leaves the School, but is instead worked with ‘online’ via the VLE or EPortal, then the utmost care should be taken that the security of the student information is maintained. Do not leave data readily accessible on-screen. Where practical school data should be stored on school systems – rather than 3rd party external providers such as ‘Drop-box’ or ‘SkyDrive’.</td></tr>
<tr><td colspan="4">Staff passwords for the main system should be shared with no-one.</td></tr>
<tr><td colspan="4">Staff passwords for the main system will be ‘force-changed’ every year</td></tr>
<tr><td colspan="4">No student should be allowed to work at a computer logged in with a staff log-in.</td></tr>
<tr><td colspan="4">Even when passwords are regularly changed, they should reflect higher levels of complexity, usually embodying at least eight characters, with a mix of upper and lower-case text and numbers. It should not be guessable by anybody who knows you well.</td></tr>
<tr><td colspan="4">Any comments written about students – particularly in SIMS (or equivalent) negative and positive events – need to be of the type that as a member of staff you would be willing to publish to a parent.
Personal judgements / emotive comments / pejorative words about students should be avoided.
Comments concerning one student’s events should NOT mention other students.
Comments should focus on factual events where possible.
The highest possible standards of personal literacy should feature – especially in circumstances where inaccurate grammar or spelling errors could create ambiguity</td></tr>
<tr><td>Support</td><td colspan="3">Advice Available:
Comment suitability – your Leadership Team or Line Manager
The use of password-protection for files - the ICT Support Team
Accessing student data ‘remotely’ – the ICT Support Team & TPP
What to do if you believe student personal information has been compromised: TPP</td></tr>
</table>

Appendix 6 - Key Information for Parents

National Online Safety for Children: https://nationalonlinesafety.com/about

Internet Matters: Helping Parents to keep their children safe online; https://www.internetmatters.org/

NSPCC: Safety online: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

CEOP: Child exploitation and online protection: police online safety links: https://www.ceop.police.uk/Safety-Centre/

Cyber Choices Programme:

https://www.eastmidlandscybersecure.co.uk/cyber-choices

Appendix 7 - Technical Systems to support e-Safety

The School Network Management Company will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented.

There will be regular reviews and audits of the safety and security of school ICT systems

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to nominated senior leader.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school has provided appropriate user-level filtering through the use of professional level filtering software.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the nominated senior leader.
- Requests from staff for sites to be added or removed from the filtered list will be actioned by the Network Manager (or other person)
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- Appropriate security measures are in place protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc, from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system
- The school infrastructure and individual workstations are protected by up to date virus software