Melrose Education
SCHOOL

THE LEARNING CENTRE
TLC

E-SAFETY Policy

Reviewed by:	Andrew Patterson, Compliance Manager
Date:	1 August 2023
Last reviewed on:	01 September 2022
Next review due by:	31 July 2024
Version control:	1
Approved by:	Tracey Storey, CEO

Contents

Aims
Our school aims to:

- Have robust processes in place to ensure the e-safety of learners, staff, volunteers, and SAP members.
- Identify and support groups of learners that are potentially at greater risk of harm online than others.
- Deliver an effective approach to e-safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Acceptable Behaviour
We expect our employees to:

- comply with current legislation.
- use the Internet/email in an acceptable, reasonable, and professional way.
- not engage in any prohibited activity online.
- not visit any websites or carry out any activity online which would be inappropriate in a business environment – remember many websites use cookies or other software which tracks website activity and is traceable to the company.
- not create unnecessary business risk to the company by their misuse of the Internet/email.
- not use the Internet/email facilities within the sites of Facebook, MSN or equivalent during working hours – this is a disciplinary offence – please refer and adhere to the social media policy and social networking guide for staff.

If you are issued with any equipment, such as a laptop, computer, mobile phone with Internet or email facility you should take all reasonable steps to ensure the safekeeping of both the equipment and any data either stored or displayed on any such device. If any equipment is lost, damaged or stolen because of your negligence we may deduct the cost, or partial cost, of the repair or replacement of any items. We may also invoke the disciplinary procedure. Please refer to the GDPR policy.

Unacceptable Behaviour
The following is deemed unacceptable use or behaviour by employees:

- Failing to meet job responsibilities by excessive personal use of the Internet/email during business hours.
- Using the company communications systems to set up personal businesses or send chain letters or other inappropriate messaging.
- Forwarding of company confidential messages to external locations or non-company personnel.
- Accessing or attempting to access confidential or sensitive company material unless authorised to do so.
- Distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene, or illegal.
- Distributing, disseminating, or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist, ageist or racist.
- Distributing, disseminating, or storing discriminatory, harassing, derogatory, or insulting materials.
- Accessing copyrighted information in a way that violates the copyright.
- Breaking into the system or unauthorised use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, or religious platforms.

- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the Company network.
- Modifying or removing existing systems, programmes, information, or data.
- Using Company programmes or software for any unauthorised use.
- Uploading, downloading, or opening or distributing unauthorised software.
- Generating or otherwise participating in the distribution of a computer virus.
- Using Company computers, computer equipment or internet to participate in online gambling of any kind.

The 4 key categories of risk

Our approach to E-Safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so.

Other legal frameworks supporting e-safety:

- The Computer Misuse Act 1990 (sections 1-3)
- Copyright, Design and Patents Act 1988
- General Data Protection Regulations 2018
- Malicious Communications Act 1988 (section 1)
- Obscene Publications Act 1959 and 1964
- Public Order Act 1986 (sections 17-29)
- Protection of Children Act 1978 (section 1)
- Protection from Harassment Act 1997
- The Equality Act 2010

- Regulation of Investigatory Powers Act 2000
- Sexual Offences Act 2003
- The Children Act 1989
- The Childcare Act 2006

Roles and Responsibilities

Melrose Senior Management Team

The Melrose SMT has overall responsibility for monitoring this policy and holding the principals to account for its implementation.

The Melrose SMT will ensure all staff undergo e-safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Melrose SMT will also ensure all staff receive regular e-safety updates (via email, e-bulletins, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Melrose SMT will co-ordinate regular meetings with appropriate staff to discuss e-safety, requirements for training, and monitor e-safety logs as provided by the designated safeguarding lead (DSL).

The Melrose SMT will ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Melrose SMT will ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The member of the Melrose SLT who oversees E-Safety is Henrietta Jordan, Regional Schools Director. The ICT Manager is Xuper Limited, our external ICT provider.

All members of the Melrose SMT and the schools' SLT will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that E-Safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including e-safety, is adapted for vulnerable children, victims of abuse and some learners with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

Principal
The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead
Details of the school's designated safeguarding lead (DSL) and deputies are set out in our safeguarding and child protection policy as well as relevant role analyses/job descriptions.

The DSL takes lead responsibility for e-safety in school, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the principal and directors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the principal, ICT manager and other staff, as necessary, to address any e-safety issues or incidents.
- Managing all e-safety issues and incidents in line with the school's safeguarding and child protection policy.
- Ensuring that any e-safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on e-safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on e-safety in school to the principal and directors.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including e-safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The ICT Manager - Xuper and Net Sweeper
The ICT Manager is an external support person from Xuper Limited and is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any e-safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

All Staff and Volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- **To never use any personal mobile devices in school hours on the school premises**
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3) and ensuring that learners follow the school's terms on acceptable use (appendices 1 and 2).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by emailing both the DSL and Xuper.
- Following the correct procedures by contacting the DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any e-safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- Never using their own personal mobile phone to process personal data or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots.
- Not adding their school email address to their personal phone or personal device – this is expressly forbidden.

This list is not intended to be exhaustive.

Parents and Carers
Parents and carers are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).
- Not to use mobile device or take photographs while one the school grounds.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics - Childnet International
- Parent resource sheet - Childnet International

Visitors and Members of the Community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they must agree to the terms on acceptable use (appendix 3).

Educating Learners About E-Safety
Learners will be taught about e-safety as part of the curriculum:

All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, learners will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Learners in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, learners will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.

Learners in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, learners will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared, and used online.
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including e-safety, will be adapted for vulnerable children, victims of abuse and some learners with SEND.

Educating Parents and Carers About E-Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

E-safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to e-safety, these should be raised in the first instance with the principal and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the principal.

Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, directors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among learners, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices

The principal, and any member of staff authorised to do so by the principal as set out in the behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners, and/or,
- Is identified in the school rules as a banned item for which a search can be carried out, and/or,
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other learners and staff. If the search is not urgent, they will seek advice from DSL or principal.
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the learner's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data, or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or.
- The learner and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and

confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of learners will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use of the Internet in School

All learners, parents/carers, staff, volunteers, and directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners, staff, volunteers, directors, and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Learners Using Mobile Devices in School

Learners may bring mobile devices into school but are not permitted to keep them on their person. All mobile phones and smart watches must be handed it at the start of each day. Phones will be returned at the end of the day to learners.

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff Using Mobile Devices in School

Staff are not permitted to use their personal mobile phones, devices, or smart watches in school. Any breach of the acceptable use agreement by a staff will trigger disciplinary action in line with the staff disciplinary process.

Staff Using Company Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the principal or Xuper.

Use of social media
You are absolutely forbidden from accessing social media for personal purposes whilst at work, whether on our computer equipment or your own. You must not make any statements regarding your employment or workplace on social media. You must not make any derogatory comments regarding our business, our employees, our children, our parents, our suppliers or any other person or business connected to the company. Your online profile must not contain the company's or school's names. You must not be friends with parents on social media. Please refer to the social media Policy.

Security
The security of our systems and data is of great importance to the company. If it is compromised, it could harm our business or expose it to the risk of harm. To prevent this from occurring, you are required to comply with the security measures detailed below.

Unauthorised Software - Software other than that provided by the company is not to be downloaded or installed onto company computers unless specifically authorised by your principal.

External Devices and Equipment - No external devices or equipment should be attached to our computers or computer equipment without the prior approval of your principal.

Computer Viruses - Whilst the company has anti-virus software and spam filters in place, it is still expected that employees will take reasonable care to ensure that our systems do not become infected. If you are suspicious that an email or an attachment may have a virus, you should not open it. You should report it to your principal immediately. If you become aware of a virus or any other programme in our computer system that could cause harm, whether to the computer system itself, its security, or our data, you must report this immediately to your principal.

Smartphone and Tablet Applications - If you have been provided with a smartphone or other portable internet enabled device, you must not download or install any applications on to it without authorisation from your principal. Any applications you are authorised to download must be obtained from an approved source, irrespective of their availability elsewhere.

Confidential Passwords - Passwords are confidential and must not be given to another person without prior permission from your principal. Your principal must be provided with all passwords, including changes made, to ensure business continuity in the event of your unexpected absence from the business.

Securing Your Computer Terminal/Computer Device - You are required to secure your computer terminal if you are leaving it unattended. You must either log off or lock your system. This is to maintain the security of our systems and data. If you are using a laptop computer or any other mobile computing device, it is your responsibility to ensure that it is always kept secure. Care must be taken whilst away from the workplace. All mobile computing devices must be password protected. When it is not actively in use, you must

switch off or lock your device to prevent unauthorised access being gained to our systems or data. In the event of loss or theft of a device, you must report this immediately to your principal. Please also see the clear desk policy.

External Hard-Drive/USB/Memory Sticks - You are permitted to use memory sticks to store information when it is required by your role or by the company. Any information stored on a memory stick must be secure; this means it must be password protected with a strong password. You are responsible for ensuring that the memory stick is not lost or stolen whilst in your possession. If loss or theft does occur, you must immediately report this to your principal and provide a description of the information on the device.

Emails

The Company recognises that email is a useful business tool. However, it is crucial that it is always used in a professional manner, whether being sent from a computer or mobile computing device such as a smartphone or tablet. All employees are required to comply with the rules set out below.

Appropriate Use of Emails - You should correspond by email only when it is appropriate for you to do so. In any email sent in the course of employment you must ensure that:

- Your tone and content are appropriately professional.
- You identify yourself in an appropriate manner.
- You include the Company's standard disclaimer when sending emails.

Confidential Information - You are responsible for ensuring that you do not use email to reproduce, replicate, duplicate or distribute confidential or sensitive Company information to an inappropriate party. You are strictly prohibited from transferring confidential or sensitive information to your personal email account.

Creating Contractual Commitments - It is important to remember that contracts and contractual obligations can be created by email. You must not create a contract or any contractual obligations with a third party unless it is the Company's intention to do so, and you have the appropriate authority. If you require further information regarding this, please contact your principal.

Use of Emails in Court Proceedings - Emails can be disclosed in legal proceedings. Employees must bear this in mind when drafting, responding to, or forwarding emails. Even if emails are deleted, it is likely that they are recoverable and as such capable of being disclosed.

Group Emails - *The use of the BCC (blind carbon copy) function to protect confidential contact information of recipients in a group email is prohibited. This is due to the large margin for error and risk associated with this function, which could result in a breach of the GDPR. Speak to your principal about the most appropriate way to send group emails if this is required.*

Jokes - Using email for the receipt and distribution of jokes and banter is not permitted. What may seem like a joke to you may be offensive to someone else.

Junk Mail (Spam) and Chain Emails - Sending and responding to junk email chain letters/emails is forbidden.

Political and Charitable Donations - You are prohibited from using email to request or respond to a request for political or charitable donations.

Managing Your Email Account - It is your responsibility to ensure that your inbox is managed effectively, including ensuring you have sufficient space to enable you to always receive emails.

Emails should be responded to on a same day/next day basis. If a longer period is required to provide a substantive response, an acknowledgement must be sent same day/next day with an indication of the timeframe for responding fully.

You must ensure an auto response/ 'out of office' is enabled when you are out of the office, or otherwise unable to respond promptly to emails. If you are unsure who to forward your emails to in your absence, contact your principal.

The 'out of office' message must be professional and should include the following information:

- the date(s)/time you will not have access to your emails.
- the date(s)/time when you will next be contactable and will be able to respond.
- The name and contact details of the person who will be dealing with your emails in your absence.

If necessary for business purposes, the Company may access your emails in your absence.

How the School will Respond to Issues of Misuse
Where a learner misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure learners can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include e-safety, at least every 2 years. They will also update their knowledge and skills about e-safety at regular intervals, and at least annually.

Directors and SAP members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding and child protection policy.

Monitoring Arrangements

Staff

Melrose Education and its subsidiaries accept that the use of the Internet/email is a valuable business tool. However, misuse of these tools can have a negative impact upon employee productivity and the reputation of the business.

The company's Internet, cloud storage and email resources are provided for business purposes only. Therefore, the company maintains the right to examine any systems and inspect any data recorded.

To ensure compliance with this policy, the company also reserves the right to use monitoring software to check upon the use and content of Internet use and emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with employees.

Monitoring may be undertaken for the following reasons although this list is not exhaustive:

- To prevent or detect crime.
- To comply with legal obligations.
- To monitor compliance with this and other company policies.
- To monitor quality of work.
- To investigate alleged or suspected wrongful acts.

Learners

The DSL logs behaviour and safeguarding issues related to e-safety. An incident report log can be found in appendix 4.

Sanctions
Failure to comply with this policy will result in disciplinary action being taken in accordance with the company's disciplinary policy. This may lead to your dismissal.

Links with other Policies
This e-safety policy is linked to our:

- Safeguarding and child protection policy
- Behaviour policy
- Staff disciplinary procedures
- GDPR policy

Appendix 1: KS1 Acceptable Use Agreement (Learners and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of Learner	
School	

When I use the school's ICT systems (iPad and computers) and access the internet in school I will:

- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use.
- Tell my teacher immediately if:
  - I click on a website by mistake.
  - I receive messages from people I don't know.
  - I find anything that may upset or harm me or my friends.
- Use school computers for schoolwork only.
- Be kind to others and not upset or be rude to them.
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my hardest to remember my username and password.
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address, or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network.
- Check with my teacher before I print anything.
- Log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signature of Learner	
Date	

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet and will make sure my child understands these.

Signature of Parent/Carer	
Date	

Appendix 2: KS2, KS3 And KS4 Acceptable Use Agreement (Learners and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of Learner	
School	

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (iPad or computers) and access the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission.
- Keep my usernames and passwords safe and not share these with others.
- Keep my private information safe at all times and not give my name, address, or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer when I've finished working on it.

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Create, link to, or post any material that is pornographic, offensive, obscene, or otherwise inappropriate.
- Log in to the school's network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it at the start of the day to my teacher or at reception.
- I understand I am not allowed to have a mobile phone or smart watch or tablet in school.

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signature of Learner	
Date	

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet and will make sure my child understands these.

Signature of Parent/Carer	
Date	

Appendix 3: Acceptable Use Agreement (Staff, SAP Members, Volunteers and Visitors)

Staff Acceptable Use of Technology Declaration

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Melrose Education and its subsidiaries/schools IT systems in a professional, lawful, and ethical manner. In line with KCSIE 2023, all staff must understand and abide by the requirements of the statutory legislation.

To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for children, they are asked to read and understand KCSIE 2023, the relevant company policies, and sign the Staff Acceptable Use of Technology Declaration.

This declaration is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however it will help ensure that all staff understand Melrose Education's expectations regarding safe and responsible technology use and can manage the potential risks posed. This will also help to ensure that Melrose Education's systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

- I understand that this declaration applies to my use of technology systems and services provided to me or accessed as part of my role within Melrose Education both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data, and data storage and online and offline communication technologies.
- I understand that Melrose Education's Staff Acceptable Use of Technology Declaration should be read and followed in line with the Melrose Education staff Employee Handbook and E-Safety – Use of Computers, Internet and Email Policy, and E-Safety – Acceptable Use of Technology Policy.
- I am aware that this declaration does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Melrose Education ethos, Melrose Education's staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Melrose Education's Devices and Systems

- I will only use the equipment and internet services provided to me by Melrose Education, for example Melrose or school provided computers, smart TVs, laptops, tablets, mobile phones, and internet access, when working with children/learners.
- I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Personal use of school IT systems and/or devices by staff is not allowed and disciplinary action will be taken if this requirement is not adhered to.

Data and System Security

- To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
- I will use a 'strong' password to access Melrose Education or school systems. A strong password has numbers, letters, and symbols, with eight or more characters, does not contain a dictionary word and is only used on one system.
- I will protect the devices in my care from unapproved access or theft, for example by not leaving devices visible or unsupervised in public places.
- I will respect Melrose Education system security and will not disclose my password or security information to others.
- I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the principal/SLT.

- I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the principal**.**
- I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Melrose Education GDPR and any other information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by Melrose Education.
- I will not keep documents which contain Melrose Education related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. I will use the school approved cloud-based storage platform to upload any work documents and files in a password protected environment.
- I will not store any personal information on the Melrose Education IT system, including Melrose Education laptops or similar device issued to members of staff, which is unrelated to Melrose Education activities, such as personal photographs, files, or financial information.
- I will ensure that Melrose Education owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will not attempt to bypass any filtering and/or security systems put in place by Melrose Education or its schools.
- If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the principal as soon as possible.
- If I have lost any Melrose Education related documents or files, I will report this to the principal and/or school Designated Data Lead as soon as possible.
- Any images or videos of children will only be used as stated in the E-Safety – Acceptable Use of Technology Policy.
    - I understand images of children must always be appropriate and should only be taken with Melrose Education provided equipment and taken/published where children/learners and their parent/carer have given explicit consent.

Teaching and Learning Practice

- I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of children/learners, as outlined in the E-Safety – Acceptable Use of Technology Policy.
- I have read and understood the E-Safety – Use of Internet, Computers and Email, the E-Safety – Acceptable Use of Technology policy and the social media Policy which covers expectations regarding mobile technology and social media.
- I will promote online safety with the children/learners in my classroom and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used in the school.
    - creating a safe environment where children feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any children/learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with children/learners is appropriate.
- I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL.

- I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Use of social media and Mobile Technology

- I have read and understood the E-Safety – Acceptable Use of Technology Policy, social media Policy, and Social Networking Guide for Staff – Protecting your Digital Footprint, which covers expectations regarding staff use of mobile technology and social media.
- I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the Employee Handbook, when using Melrose Education and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    - I will take appropriate steps to protect myself online when using social media as outlined in the Social Networking Guide for Staff – Protecting your Digital Footprint.
    - I am aware of Melrose Education's expectations with regards to use of personal devices and mobile technology, including mobile phones and Smartwatches as outlined in the E-Safety – Acceptable Use of Technology Policy.
    - I will not discuss or share data or information relating to children/learners, staff, Melrose Education or its subsidiaries' business or parents/carers on social media.
    - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the Employee Handbook and the law.
- My electronic communications with current and past children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries:
    - I will ensure that all electronic communications take place in a professional manner via Melrose Education/school approved and/or provided communication channels, such as a Melrose Education or school email address or telephone number.
    - I will not share any personal contact information or details with children/learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past children/learners and/or parents/carers.
    - If I am approached online by a child/learner or parents/carer, I will not respond and will report the communication to my principal and the Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with this AUD will be discussed with the DSL and/or principal.
- If I have any queries or questions regarding safe and professional practise online either in Melrose Education, its schools, or off site, I will raise them with the DSL and/or the principal.
- I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
- I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
- I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Melrose Education or its subsidiaries into disrepute.

Policy Compliance

I understand that Melrose Education may exercise its right to monitor the use information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of children/learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

Policy Breaches or Concerns

- I will report and record concerns about the welfare, safety or behaviour of children/learners or parents/carers to the DSL in line with Melrose Education's Safeguarding and Child Protection Policies.

- I will report concerns about the welfare, safety, or behaviour of staff to the principal, in line with Melrose Education's Safeguarding and Child Protection Policies.
- I understand that if Melrose Education or its subsidiaries believe that unauthorised and/or inappropriate use of company or school systems or devices is taking place, Melrose Education may invoke its disciplinary procedures as outlined in the Employee Handbook.
- I understand that if Melrose Education believe that unprofessional or inappropriate online activity, including behaviour which could bring the Company or school into disrepute, is taking place online, they may invoke its disciplinary procedures as outlined in the Employee Handbook.
- I understand that if Melrose Education suspects criminal offences have occurred, the police will be informed.

I have read, understood, and agree to comply with the Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off school site.

Employee Name			
Job Title			
School			
Date of Signing	***Autumn term***	**Employee Signature**	
Date of Signing	***Spring term***	**Employee Signature**	
Date of Signing	***Summer term***	**Employee Signature**	

Appendix 4: Online Safety Incident Report Log

E-SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**