ONLINE, EMAIL AND SOCIAL MEDIA SAFETY POLICY

The ELKOLET Centre, Mill Lane, Alton, GU34 1BD

T: 01420 86980 W: www.elkolet.com

E: info@elkolet.com

Reviewer	Paula Knowles
Review Date	Sept 2024
Next Review Date	Sept 2025

Contents

Purpose of Policy

This policy aims to:

- Set out expectations for all ELKOLET's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help staff and volunteers working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of ELKOLET, supporting the charity's ethos, aims and objectives, and protecting the reputation of ELKOLET and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

Scope

This policy applies to all members of the ELKOLET community (including staff, trustees, volunteers, contractors, students/pupils, parents/carers, visitors, and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their role. ELKOLET will regularly review and update its filtering and monitoring practices to ensure they remain effective and in compliance with applicable laws and regulations. By using the Filtering and Monitoring Review Checklist, ELKOLET can ensure we are meeting the required standards of cyber security and filtering and monitoring.

Roles and Responsibilities

ELKOLET is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of ELKOLET.

Director of Education and Family Support

- Foster a culture of safeguarding where online safety is fully integrated into whole-charity safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff and volunteers.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance

- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the charity's provision follows best practice in information handling; work with the DSL and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the charity implements and makes effective use of appropriate IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff and volunteers aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff who carry out internal technical online-safety procedures
- Ensure trustees are regularly updated on the nature and effectiveness of the charity's arrangements for online safety
- Monitor the use of charity technology, online platforms, and social media presence and that any misuse/attempted misuse is identified and reported in line with charity policy.
- Utilise the DfE advice for schools: teaching online safety in schools

Designated Safeguarding Lead

The DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education, 2024:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure "an effective whole school (…) approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Director of Education and Family Support and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety

- Review and update this policy, other online safety documents and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the trustees.
- Ensure that online safety education is embedded across the curriculum and beyond
- Promote an awareness and commitment to online safety throughout the charity's community, with a strong focus on parents, who are often appreciative of support in this area, but also including hard-to-reach parents
- Communicate regularly with the designated safeguarding trustee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring
- Ensure all staff and volunteers are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with trustees and ensure staff are aware.
- Facilitate training and advice for all staff:
    - all staff must read at least KCSIE Part 1
    - all those who do not work directly with children must read either Part 1 or Annex A
    - cascade knowledge of risks and opportunities throughout the organisation

Trustee Board

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2024):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- "Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. (…) The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).".
- Support the charity in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at trustee meetings
- Work with the Director of Education and Family Support and DSL to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; all not working directly with children have read Annex A.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (…)) at induction. The training should be regularly updated. Induction and training should be in line with any advice from local safeguarding partners."

- "Ensure appropriate filtering and monitoring systems are in place [but…] be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).".

All Staff

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Leads (DSL) are, Paula Knowles and Julie Mathers
- Read Part 1 of Keeping Children Safe in Education 2024.
- Read and follow this policy in conjunction with the charity's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with charity procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct within the Employee Handbook
- Notify the DSL if policy does not reflect practice in the charity and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology, etc) on site or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask a DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in recreational/communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible, and professional behaviours in their own use of technology. This includes outside the charity hours and site, and on social media, in all aspects upholding the

reputation of the charity and of the professional reputation of all staff. More guidance on this point can be found in this Professional Reputation guidance for schools.

Volunteers and Contractors

- Read, understand, sign, and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible, and professional behaviours in their own use of technology
- Volunteers must read KCSIE 2024 Part 1.

Students

- Read, understand, sign, and adhere to the student guidelines code of conduct.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of the charity and realise that the acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at ELKOLET or outside of the charity if there are problems

Parents/Guardians/Carers

- Read, sign, and promote the parental guidelines and read the pupil guidelines and encourage their children to follow it.
- Consult with the charity if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the charity staff, volunteers, trustees, contractors, pupils, or other parents/carers.

Education

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Relationships education, relationships and sex education (RSE)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all activities, both outside the classroom and within the curriculum,

supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology, etc) on site, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At ELKOLET, we recognise that online safety and broader digital resilience must be a thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns about a child

It is vital that all staff recognise that online safety is a part of safeguarding as well as a curriculum strand.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead, to contribute to the overall picture or highlight what might not yet be a problem.

Support staff and volunteers will often have a unique insight and opportunity to find out about issues first in recreational and communal areas (particularly relating to bullying and sexual harassment and violence).

ELKOLET's procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including sanctions)

ELKOLET commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside the Alternative Provision and outside (and that those from outside will continue to impact on students). All members of the charity are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the charity's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day.

Any concern/allegation about staff misuse is always referred directly to the Director of Education and Family Support, unless the concern is about the Director in which case the compliant is referred to the Chair of Trustees. Staff may also use the NSPCC Whistleblowing Helpline.

The charity will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education 2024' and 'Data protection in schools' toolkit 2024, which the DSL will seek to apply. This quote from the KCSIE 2024 is useful for all staff:

"The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

The DSL will usually decide if personal data needs to be shared. They should make sure they record:

- who they're sharing that information with
- why they're sharing the data
- whether they have consent from the student, parent or guardian

All students, staff, trustees, volunteers, contractors, and parents/carers are bound by the Charity's data protection policy and agreements, which can be found here https://www.elkolet.com/policy-center .

The Director of Education and Family Support, DSL and trustees work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Filtering

Access to the administrative interface for all filtering and monitoring systems are protected with multi factor authentication. All firmware is kept up to date and regularly checked by the appointed IT persons. All unauthenticated connections are blocked by default.

Devices which are used by students are not allowed off-site. The devices remain on the ELKOLET premises and only connected to the ELKOLET provided Wi-Fi to allow for protection and monitoring.

MFA is enabled on all staff and administrative accounts that access sensitive or network data to ensure the protection of said data from outside malicious threats.

Internet Filtering

ELKOLET employs an internet content filtering system to restrict access to inappropriate, harmful, or malicious websites and content. This system is continuously updated to adapt to evolving online threats.

The content filtering system operates at both the ELKOLET network level and on individual devices issued by us. It is configured to block access to websites, web applications, and online platforms that are not deemed suitable for educational purposes.

Requests for unblocking specific websites for educational purposes should be directed to the designated IT administrator, who will review and, if appropriate, unblock the requested content.

Email Filtering

ELKOLET utilises Microsoft 365 for Education. This service's email system incorporates filtering mechanisms to minimize the risk of phishing attacks, spam, and malicious email content.

Students and staff are encouraged to report any suspicious emails to the IT department for investigation and potential action.

Monitoring

The charity reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken. There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Network Monitoring

ELKOLET's network is continuously monitored for unusual or suspicious activity that may pose a threat to the security and well-being of students and staff.

Network logs are regularly reviewed by the appointed IT person to detect any unauthorized access or breaches of security.

Any unusual or suspicious activity discovered during network monitoring will be promptly brought to the attention of the DSL, subsequently investigated, and appropriate action will be taken, which may include reporting the incident to the relevant authorities.

Device Monitoring

All ELKOLET-issued devices, including laptops and tablets, are subject to monitoring to ensure they are used for educational purposes and in accordance with ELKOLET's policies.

Monitoring of devices may include tracking software, which helps in locating lost or stolen devices.

Monitoring is not intended to infringe upon individuals' privacy but to ensure a safe and secure learning environment.

No application downloads on ELKOLET devices is allowed in configuration to ensure no malicious or inappropriate applications are being used by students. Should this be required, the request to the IT persons and DSL shall be submitted and an administrator account can see to the necessary changes.

Within the monitoring process, all devices are regularly check by the appointed IT persons to ensure all applications and operating systems and software is up-to-date to reduce the vulnerability of applications and devices. All software and applications are enabled for automatic updates to reduce the likelihood of a missed update due to human error.

Digital Communication Monitoring

ELKOLET may monitor digital communications conducted on ELKOLET-owned platforms, such as email and messaging systems, to ensure compliance with our policies and to prevent cyberbullying, harassment, grooming or other inappropriate conduct.

Monitoring of digital communication will be conducted discreetly and with respect for privacy, only as necessary to address specific concerns or incidents.

Property

Staff, volunteers, and students should treat any property belonging to the charity with respect and reasonable care and report any faults or breakages to a member of staff.

Viruses

Staff, volunteers, and students should be aware of the potential damage that can be caused by computer viruses. Staff, volunteers, and students must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers and laptops are password protected. Passwords are changed on a regular basis.
- Students should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.
- Do not make deliberate attempts to disrupt or damage the charity network, any device attached to it or any data stored on it or transmitted across.
- Do not alter charity hardware in any way.
- Do not knowingly misuse headphones or any external devices e.g. printers, mouses.
- Do not eat or drink while using the computer.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation.

Internet

ELKOLET recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for charity related activities only. ELKOLET monitors the use of the Internet.

ELKOLET's internet system has a filtering and monitoring system run which monitors and filters all website access against pre-set policies. Any inappropriate material, whether it be sexual, violent, extremist, or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the school Designated Safeguarding Lead, as to the inappropriate material being accessed.

Viewing, retrieving, or downloading of any material that the charity considers inappropriate will result in appropriate disciplinary action.

Electronic communications

Email

Staff and students use Outlook from Office 365 with the relevant licenses.

This system is fully auditable, trackable, and manageable. This is for the mutual protection and privacy of all staff, students, and parents/carers, as well as to support data protection.

General principles for email use are as follows:

Email and the chat functionality of Microsoft Teams are a means of electronic communication to be used between staff and students, staff and parents/carers (in both directions). Use of a different platform must be approved in advance by the Director of Education and Family Support. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Director Headteacher (if by a staff member).

Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Director (the circumstances of the incident will determine whose remit this is) should be informed immediately.

Staff or student personal data should never be sent/shared/stored on email.

- If data needs to be shared with external agencies, encryption systems are used
- Internally, staff should use the charity network, including when working from home when remote access is available via charity-run Office365.

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the charity into disrepute or compromise the professionalism of staff.

Staff and students are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour

apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

WhatsApp Business

ELKOLET and TKW utilise WhatsApp Business via a dedicated company phone to communicate with parents/guardians as it offers a fast, convenient, and secure way to stay connected. With WhatsApp, we can quickly share important updates, answer questions, and provide support, ensuring that parents/guardians are always informed and engaged.

WhatsApp business offers several safeguard protections to ensure the safety of users including:

- End-to-end encryption- All messages, calls, and media sent through WhatsApp Business are protected by end-to-end encryption. This means only the sender and the recipient can read the messages, and not even WhatsApp itself has access to the content. It ensures that messages are secure from potential interception.
- User control over data- WhatsApp Business gives users control over certain aspects of their data, including blocking or reporting business contacts if they feel uncomfortable with the interaction or suspect a breach of privacy.
- Data download option- Users can request to download their account information and settings from WhatsApp.
- Two-step verification- WhatsApp Business offers two-step verification as an additional security measure. This adds an extra layer of protection by requiring a PIN in addition to the phone number for logging into the account.
- Business verification- ELKOLET is a verified business and as such all staff contacts related to our organisation have a green badge displayed next to the name. This badge signifies that WhatsApp has confirmed that the phone number belongs to a legitimate business, which helps to identify genuine businesses and avoid scams.
- Data minimisation- WhatsApp Business does not store messages on its servers after they are delivered. Unsent messages are kept on the server for up to 30 days, after which they are automatically deleted if undelivered. This ensures that data is not stored unnecessarily.
- Transparency with interactions- WhatsApp allows users to see the business name, phone number, and other business information such as physical location or website. This transparency helps users know who they are communicating with and ensures a certain level of trust.
- Compliance with GDPR regulations- WhatsApp has implemented mechanisms for handling data protection requests, ensuring transparency, and providing users with options to manage their data.
- Data encryption for backups- As we back up our chats, WhatsApp offers encrypted backups to prevent unauthorized access. This feature ensures that even stored messages are protected from potential breaches. To see how long we retain data for, please see our Data Protection policy.
- Security against malware and phishing- WhatsApp has built-in protections against common cybersecurity threats like malware and phishing. WhatsApp monitors for suspicious links and behaviours, alerting users to potential risks in their conversations.

- Limited data sharing with meta- While WhatsApp Business does share some metadata with its parent company Meta (formerly Facebook), such as the phone number, registration details, and interactions with other businesses, the content of messages remains private due to encryption. Users are also informed about this data sharing through WhatsApp's privacy policy.

To find out more on WhatsApp safety features visit https://business.whatsapp.com/trust-and-safety

To read Meta's privacy policy visit https://www.facebook.com/privacy/policy

Cloud platforms

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our Data Protection Policy.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and students safe, and to avoid incidents. The network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that student data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Staff and students are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or student data
- Student images/videos are only made public with parental permission
- Only charity-approved platforms are used by students or staff to store work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which young people, parents/carers and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes, and it is an important element of school life.

At ELKOLET we feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within ELKOLET, and it is employed routinely in many ways, for example; record keeping, displays, special events, teachers' lessons and the student's own work.

On occasions photos are also used for the Press, charity website, charity Facebook page and other promotional purposes.

Young people will only be named in photographs that are displayed within the charity. We will not provide their full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images.

Taking Photographs and Video

All parents/carers are asked to give consent for photography of their child by completing a permission slip that is held on file. A register is kept of children who must not be included in press, website, or any other photographic image, still or moving.

All reasonable measures will be taken to ensure that no child on the register is photographed or videoed by a visitor to the charity or while on an educational visit. The exception to this may be photographs taken by parents/carers at events such as award services.

Images taken by school staff

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.

All images taken must be deemed suitable without putting the child in any compromising positions that could cause embarrassment or distress.

Under no circumstances will a camera be allowed into the bathroom areas.

Photographs taken as records of events or for educational purposes may be displayed around the charity's premises. They are then archived or shredded after use.

Photographs are not exchanged with anyone outside school or removed for private use by any employee or volunteer.

Images taken by adults other than school staff

When a commercial photographer/filmmaker is used we will;

- Provide a clear brief
- Issue Identification
- Inform parents/carers and students
- Obtain consent
- Not allow unsupervised access to students

Images taken by students

Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include trustees, parents /carers or younger children.

Students are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Should the school learn about any inappropriateness of image use involving our students, staff or volunteers, we will immediately act and report it as we would for any other child protection issue

Social media

ELKOLET's SM presence

ELKOLET works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the charity online).

Negative coverage almost always causes some level of disruption. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the charity and to respond to criticism and praise in a fair, responsible manner.

ELKOLET is responsible for managing our Facebook/LinkedIn accounts and checking our Google reviews.

Staff, students' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a charity, we accept that many parents/carers, staff and students will use it. However, as stated in the acceptable use policies which all members of the charity community sign, we expect everybody to behave in a positive manner, engaging respectfully with the charity and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the charity or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents/carers have a concern about the charity, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the charity complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the

matter, but can cause upset to staff, students and parents/carers, also undermining staff morale and the reputation of the charity (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but ELKOLET regularly deals with issues arising on social media with students under the age of 13. We ask parents/carers to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the charity has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents/carers can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.

The charity has an official Facebook account (managed by Paula Knowles) and will respond to general enquiries about the school but asks parents/carers not to use these channels to communicate about their children.

Email and WhatsApp is the official electronic communication channel between parents/carers and the charity, and between staff and students.

Students are not allowed* to be 'friends' with or make a friend request** to any staff, trustees, volunteers, and contractors or otherwise communicate via social media.

Students are discouraged from 'following' staff, trustee, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Director, and should be declared upon entry of the student or staff member to the charity).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Director (if by a staff member).

Staff are reminded that they are obliged not to bring the charity or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the charity or its stakeholders on social media and be careful that their personal opinions might not be attributed to the charity, thus bringing the charity into disrepute.

All members of the charity community are reminded that particularly in the context of social media, it is important to comply with the policy on Digital Images and Video, outlined in the previous section, and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

Personal devices including wearable technology and bring your own device (BYOD)

Students are allowed to bring mobile phones in for emergency use and may use mobile phones during breaks. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to a placement review meeting and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made in the office, which will also pass on messages from parents/carers to students in emergencies.

Volunteers, contractors, trustees should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of students or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Director should be sought and this should be done in the presence of a member staff.

Parents/carers are asked to leave their phones in their pockets and on silent when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents/carers are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the main office.

Network / internet access on school devices

Students are not allowed networked file access via personal devices. However, they are allowed to access the charity wireless internet network for learning-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

Volunteers and contractors can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Parents/carers can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Director, and staff authorised by them, have a statutory power to search a pupil or their possessions where they have reasonable ground to suspect that the pupil may have a prohibited item. This encompasses electronic devices, including mobile phones, which can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not exclusive to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour. See our Behaviour Policy at www.elkolet.com/policy-center for more information.

Appendix A – Acceptable Use Policy

What is an AUP?

We ask all children, young people and adults involved in the life of ELKOLET to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using charity networks, connections, internet connectivity and devices, cloud platforms and social media (both when onsite and offsite).

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong, and people can get upset, but these rules should help us avoid it when possible and be fair to everybody.

Charity systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a charity device or using charity networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe.

But you should not behave any differently when you are not onsite or using your own device or home network, either. All the points in the list on this page and the next page below can be summarised as follows:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

If your parents/carers want to find out more, they can read ELKOLET's full Online, Email and Social Media Safety Policy at https://www.elkolet.com/policy-center for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.

If you have any questions about this AUP, please speak to Paula Knowles

What am I agreeing to?

1. I will always treat myself and others with respect; when I am online or using a device, I will treat everyone as if I were talking to them face to face.
2. Whenever I use a device, the internet or any apps, sites, and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
3. I consider my online reputation with everything that I post or share – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

4. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling.
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
7. If I see anything that shows people hurting themselves or encourages them to do so, I will report it on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
9. I will only use the charity's internet and any device I may be using in school for appropriate learning activities and learning, unless I have express permission to carry out recreational activities, e.g. in lunchtime or after school.
10. I understand that all internet and device use onsite may be subject to filtering and monitoring; charity-owned devices may also be subject to filtering and monitoring when used offsite, and the same expectations apply wherever I am.
11. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
12. I will not bring files onsite or download files that can harm the charity network or be used to bypass charity security.
13. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
14. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the charity, my age or learning activities, including sites which encourage hate or discriminating against others.
15. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
16. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at the charity or outside. I will stand up for my friends and not be a bystander.
17. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful, or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.

18. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions (many social media sites are 13+) and I should respect this. 18-rated games are not more difficult but are inappropriate for young people.
19. When I am at ELKOLET, I will only e-mail or contact people as part of learning activities.
20. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the charity.
21. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure, I will never open a file, hyperlink or any other attachment.
22. I will not download copyright-protected material (text, music, video etc.).
23. I will not share my or others' personal information that can be used to identify me, my family, or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
24. Live streaming can be fun, but I always check my privacy settings and know who can see what and when. If I live stream, my parents/carers know about it.
25. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.
26. I will never arrange to meet someone face to face who I have only previously met in an app, site, or game without telling and taking a trusted adult with me.
27. I will only use my personal devices (mobiles, smartwatches etc) in ELKOLET if I have been given permission, and I will never take secret photos, videos or recordings of teachers, students, or anyone else onsite.
28. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
29. I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
30. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
31. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
32. I don't have to keep a secret or do a dare or challenge just because a friend tells me to – real friends don't put you under pressure to do things you don't want to.
33. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
34. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.

35. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get in touch with Childline, The Mix, or The Samaritans.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understood these rules and agree to them.

Signed: _____ Date: _____