Online Safety Policy

RIDGEWAY EDUCATION TRUST

Approved by the Trust Board: 08 December 2020
Review date: December 2021

Purpose

This policy guidance aims to help everyone understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies. This policy sets out the principles which Ridgeway Education Trust (which for the purpose of this policy means the Trust and its associated schools) staff and pupils are expected to follow when using the Internet and social networking sites. The Internet is a fast-moving technology and it is impossible to cover all circumstances, however, the principles set out below should always be followed.

This document should be read in conjunction with the IT Acceptable Use guidelines that can be found on each school's website.

Roles and responsibilities (applicable to all users of IT Systems)

Deliberate unlawful/inappropriate material must not be viewed/stored/distributed on any Trust owned system. This can include material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to:

- be defamatory;
- be violent;
- be offensive;
- be abusive;
- be indecent or obscene;
- be discriminatory;
- incite hatred;
- constitute bullying and/or harassment; and
- breach anyone's confidence, privacy, trade secrets or copyright.

If someone has stated that they do not wish to receive emails from you then you must refrain from sending further emails to them. You must not use an organisation's email systems for 'spamming' purposes (the use of email to send unwanted/junk/advertising content to multiple recipients).

Particular care should be taken whenever you choose to use your own personal technologies in a work environment and ensure that other people, including children, are not able to see personal contents which you would deem private or sensitive, keeping professional and private lives separate.

Members of staff or volunteers must only make contact with pupils using a Trust provided email account or phone number. Ensure a clear professional basis for all communications with pupils. Personal email accounts, phones and social media accounts must not be used to contact pupils unless there are exceptional circumstances. You must inform your line manager if you have had to use your own email account, phone or social media accounts to make contact with a pupil. Furthermore, students should not be emailing from their personal accounts. Please ensure students to only use a Trust provided email account when corresponding with a teacher.

It is very important that staff maintain professional relationships with pupils at all times and we feel that these may be compromised by allowing pupils access to personal information or photographs. However well we feel that we know pupils and however mature that we feel they are, it is always possible that messages may be misinterpreted by pupils and relationships may be damaged as a result. Ensure you use appropriate privacy settings.

You must ensure that your work computer account is not misused so you should not share your username or password with anyone. All internet and network use of systems may be subject to monitoring by schools and this may be traced back to you. Everyone is responsible for ensuring information systems are secure, safe and used to benefit all. You should be aware that disciplinary/civil/criminal action might arise if any user is found to be deliberately accessing illegal content. Similarly, unauthorised or deliberate illegal access to or use of data, systems or networks is prohibited and may also result in disciplinary/civil/criminal action.

It is unacceptable to publish any defamatory and/or knowingly false material about the Trust or its schools, colleagues and/or our pupils on social networking sites, ‘blogs’, ‘wikis’ or any other online publishing format. Students and employees are expected to behave appropriately when on the Internet, and in ways that are consistent with the Trust’s values and policies. It is important that the outside activities of staff and pupils do not undermine the Trust’s reputation. Furthermore, we expect that parents and carers of children at the Trust’s schools behave appropriately online and refrain from publishing any defamatory, abusive and/or false material about the Trust, its schools, staff or pupils on any online publishing format.

Roles and responsibilities (applicable to the Trust as a whole)

The Executive Headteacher is ultimately responsible for network activity and online safety in the Trust. Online safety is led by an identified person within each organisation who has designated responsibility for it. They should receive regular training to support their role. At all Trust schools the designated persons are the Designated Safeguarding Leads (DSLs) and, in their absence, the Deputy DSLs.

All schools must connect to broadband via Filtered Internet Services to reduce the risk of anyone accessing illegal/unsuitable sites. This covers all users connected to the organisation’s networks with the exception of the IT Services staff. Any user who accidentally accesses material they deem to be inappropriate on their own machine (or notices the same on others’ machines) must report this to their online safety lead officer to help protect themselves, other people and their organisation.

Ideally, all schools will encourage and develop:

- ongoing online safety training to their wider community;
- the safe use of social networking sites; and
- secure ‘guest’ access to their networks of an individual’s own learning device, be that a laptop, smartphone or portable games console.

The Trust is responsible for having practices/procedures/staffing in place to ensure that:

- all computers (and other ICT equipment) have fully up to date anti-virus and anti-spam protection;
- all software is properly licensed for use within school;
- appropriate measures are in place to prevent the bypassing of filtering or network security systems;
- devices not owned by the organisation (such as personally-owned devices) cannot connect directly to secure systems (but may connect through “guest” access systems, where available);
- all users have personal, identifiable and secure logons to network resources so that illegal/inappropriate use can be identified to a particular user. Shared passwords/logons should not be used;
- all users of their systems have regular updates where the latest information surrounding being e-safe can be shared; and

- all users are aware of how to report suspicious activity they detect to their identified esafety/safeguarding person who may then, if necessary, notify local and/or national agencies e.g. the Child Exploitation and Online Protection Agency (CEOP) and the Internet Watch Foundation (IWF) following agreed NSCB procedures.

Any device on the school premises, whether school-owned or personally-owned, must be handed over to be checked if there is a suspicion of unacceptable usage.

- All staff have the authority to confiscate and check pupils' personally-owned devices.
- Any unacceptable usage will result in confiscation and standard school behaviour policy being applied.
- If it is suspected that the unacceptable usage could require additional investigation by school or external personnel, the device will be stored securely in school until investigations are complete.

Virtual Lessons

Following the COVID-19 outbreak, the Ridgeway Education Trust schools moved to Virtual Home Learning for the majority of pupils. From September 2020, whilst schools re-opened, Guided Home Learning continues to be part of the curriculum, either as a means of providing support for individual pupils in specific circumstances, or as part of a more flexible and diverse educational offer.

Schools are continuing to develop and enhance this provision over time as expertise, training and development improves.

Ridgeway Education Trust is committed to ensuring that online safety standards are maintained in the delivery of Guided Home Learning. Alongside the provisions in the Safeguarding and Child Protection Policy and the staff Code of Conduct and Acceptable Use Agreements for staff and pupils, the guidelines below must be followed.

Providing a safe system

For the purposes of Virtual Home Learning, the following platforms must be used across Ridgeway Education Trust:

- Microsoft Teams
- Zoom
- Office 365 email
- Satchel:One
- Google Classroom (Sutton Courtenay CofE Primary School)

Teachers should record live online sessions for safeguarding purposes. When a recording is made, access is only within the RET SharePoint area.

For staff:

- Only use school approved platforms
- Keep a record/log of live online lessons – Any serious incidents should be reported in the usual manner depending on the nature of the issue
- Maintain professional conduct during live streaming – dress appropriately, consider your surroundings (background, other household members who may come into view etc.) and blur your background if necessary. Staff should mute their microphones when not in use.
- Maintain the same boundaries and insist on the same standard of behaviour as in a school setting. Make specific protocols clear at the outset, e.g. muting of microphones at appropriate times, use of the chat function, etc.

- All 1:1 teaching sessions & support and pastoral 1:1 sessions should be recorded for safeguarding purposes.

Online Safety for pupils

At Sutton Courtenay CofE Primary School, St Birinus School and Didcot Girls' School, all pupils have a series of lessons on the topic of online safety. For the primary school, these are delivered in Computer Science and PSHCE lessons and through careful liaison with parents and carers. For the secondary schools, these are delivered in Computer Science/PD lessons and in all Key Stages pupils receive assemblies on the topic and online safety messages are reinforced as part of a planned programme of assemblies.

Ridgeway Education Trust has a framework which describes the progression of skills and knowledge students should receive within the trust, with students having the opportunity to develop these skills at different ages and key stages. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it safely.

The framework focuses specifically on seven different aspects of online education, including:

1. Self-image and Identity/Online reputation
2. Online relationships
3. Online bullying
4. Managing online information
5. Health, wellbeing and lifestyle
6. Privacy and security
7. Copyright and ownership

The framework aims to support and broaden the provision of online safety education within Ridgeway Education Trust, so that it is empowering, builds resilience and effects positive culture change.

The school computer network is for educational use and pupils should not abuse this system. When accessing the network, pupils must keep their password safe and must not share it with other people. They should not attempt to access the network area of other users or attempt to gain access to unsuitable information.

IT Services across the MAT have in place various systems which are designed to automatically monitor the activity of all staff and pupils on MAT-owned devices, with the intention of detecting safeguarding concerns. These systems may extend to live screen capture and keyword scanning for all content accessed or created. Where appropriate contracted third-party safeguarding specialists, who monitor reporting against agreed criteria, will notify the school of identified concerns, including the escalation of time critical incidents via immediate telephone call.

During school, staff will guide pupils towards appropriate materials whilst accessing the Internet. Outside of school, pupils should take care regarding the use of the Internet, mobile phones and social media sites:

- They should be careful about who they share their personal contact details with. This includes email addresses and mobile phone numbers.
- They should take extra care when interacting with other people in chat rooms and online. These people may not be who they say they are.

- They should not give out personal information to people they do not know very well.
- They should never agree to meet anyone with whom they have only had contact with online.
- To help keep pupils safe, they should share the details of the people they are communicating with, online, with parents and friends.
- They must take care if accessing social networking sites such as Facebook, Twitter etc.
- They must not use social media sites to post offensive material or to make themselves vulnerable to the inappropriate actions of others.
- They should avoid using mobile phones and text messages, in an inappropriate manner, which could be interpreted as cyber-bullying by the person receiving the communication.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- They are reminded that any photograph that they allow to be taken of them, or any image which they share online or via a mobile phone, can potentially be seen by a world audience via the Internet.

If they consider themselves, or another student, to be at risk from cyber-bullying or online safety issues, they are reminded to inform an adult – either at home or school. The designated persons, with responsibility for online safety at Sutton Courtenay CofE Primary School, St Birinus School and Didcot Girls' School, are the Designated Safeguarding Leads, who can be contacted for further advice and support.

Parents/Carers

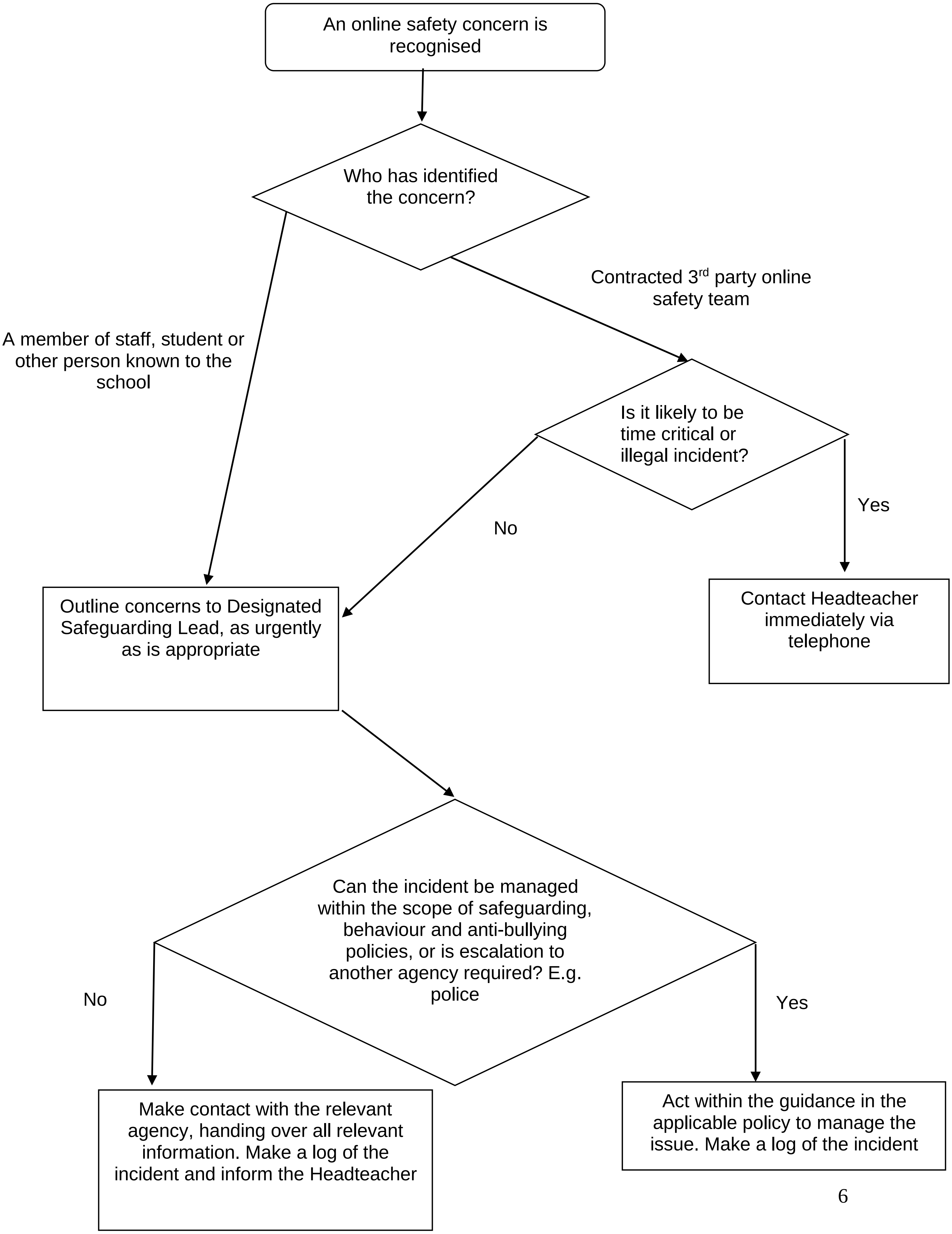
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Ridgeway Education Trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns, including Safer Internet Day.

Prevent and counter-terrorism

Ridgeway Education Trust recognises and accepts its legal responsibility to prevent young people in its care from being drawn into terrorism. All staff are trained in identifying pupils who may be at risk of being drawn into terrorism, and are also trained to challenge extremist ideas. Where a member of staff has a concern, this will be passed to the respective Designated Safeguarding Leads, where action will be taken in line with our safeguarding policy.

The Trust will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools, and that suitable filtering and monitoring is in place.

Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the Trust is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain informed advice immediately.



An online safety concern is recognised

Who has identified the concern?

A member of staff, student or other person known to the school

Contracted 3rd party online safety team

Is it likely to be time critical or illegal incident?

No

Yes

Outline concerns to Designated Safeguarding Lead, as urgently as is appropriate

Contact Headteacher immediately via telephone

Can the incident be managed within the scope of safeguarding, behaviour and anti-bullying policies, or is escalation to another agency required? E.g. police

No

Yes

Make contact with the relevant agency, handing over all relevant information. Make a log of the incident and inform the Headteacher

Act within the guidance in the applicable policy to manage the issue. Make a log of the incident