



Online Safety Policy

Date of Last Review: Autumn, 2021

Shared with all Staff: Autumn, 2021

Frequency of Review: Annually

Person responsible for review: Leadership

Date of Next Review: Autumn, 2022

The purpose of the Online Safety Policy

The purpose of this policy is to ensure that all staff, parents, councillors and children understand and follow the school's approach to Online Safety. This policy must be read alongside other policies including: the Computing Policy, the Behaviour and Relationships Policy and the Child Protection and Safeguarding Policy.

Online Safety encompasses the use of new emerging technologies, internet and electronic communications such as mobile 'phones, collaboration tools and personal publishing.

The policy highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

Writing and reviewing the Online Safety Policy

The school will appoint an Online Safety lead who will work closely with the Designated Safeguarding Team and Computing lead as the roles overlap and will work together in an Online Safety Working Group. The Online Safety Policy and its implementation will be reviewed at least annually.

Teaching and learning

Why Internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils in order to maximise learning potential.

Internet use will enhance learning

- The school internet access will be designed expressly for pupil use and will include filtering and supervision appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives and supervision for its use including access to specific, approved online materials.
- Pupils will be educated in the effective use of the internet in research, including the skills of using search engines, retrieval and evaluation. Pupils will be taught how to evaluate internet content.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

as well as being able to filter appropriate information as required for the learning.

- Should staff or pupils come across unsuitable online materials, it must be reported to the Online Safety lead.

Managing Internet Access, Information system security

- School systems' capacity and security will be reviewed regularly.
- Virus protection will be up-dated regularly.

E-mail Content and the School Website

- Pupils, when part of the curriculum, are taught how to use email in school.
- The contact details on the Greenacres' website should be the school address, email and telephone number. Staff or pupils' personal information will not be published unless a specific reason is agreed at leadership level.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Outcomes

- Photographs that include pupils will be selected carefully; those without permission will be pixelated.
- Pupils' full names will not be used anywhere on the website - particularly linked together with photographs.
- On entry to Greenacres, written permission from parents or carers will be obtained allowing children's photographs to be used.
- Pupil's outcomes can be published on the school website.

Social Networking and Personal Publishing

The school will deny access to social networking sites and students will be advised not to use these at home. Staff may have social media accounts but should not reference Greenacres within them. For specific guidance regarding 'sexting,' please refer to APPENDIX

Managing Filtering

- The school will work with the Trust, LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety lead.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Handling Online Safety Complaints

- The Head teacher will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Head teacher. Complaints of a child protection nature must be dealt with in accordance with Greenacres' Child Protection and Safeguarding Procedures.

Community Use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the Online Safety policy.

Introducing the Online Safety policy to pupils

- Parents/Carers will be asked to sign and return an 'acceptable use policy' consent form as part of the school induction procedures.
- Online safety rules are discussed with the pupils at the start of each half term. Online safety posters are posted next to all computers within classrooms ensuring all users can see them.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- Pupils receive online safety lessons and safety is embedded into everyday teaching as well as in assemblies.

Staff and the Online Safety policy

- All staff will have access to the School Online Safety Policy and its importance explained.
- Staff should be aware that internet use will be monitored; discretion and professional conduct is essential.
- School camera, iPads and mobiles phones (EYFS) will only be used to photograph children.
- Staff will ensure their personal social media accounts do not reveal their workplace or have any references to incidents within school or

- photographs of the school or people within.
- Staff will not become 'friends' with parents or children on social media.
- The maximum security settings will be activated on any social media accounts.

Enlisting Parents' Support

Parents' attention will be drawn to the School Online Safety Policy in newsletters and conversations.

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photographs should not be posted on any social network space without considering how it could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils should only invite known friends and deny access to others. · Pupils will only use their own accounts/login details for apps, websites, social media, email etc.

For further support on online safety matters (as they relate to their child's internet use beyond school), parents will be kept informed of useful websites (www.internetmatters.org and www.childnet.com/parents-and-carers).

APPENDIX 1 – Online Safety Incident Log at Greenacres

APPENDIX 2 - Overarching Risks and Definitions

APPENDIX 3 - Steps to take in the case of an incident of sexting

APPENDIX 1

Online Safety Incident Log at Greenacres 2021-22	
Reported By (Name of Staff Member):	Reported To (Head teacher, Online Safety Lead etc.):
Date:	Date:
Incident Description (Describe what happened, involving which children and/or staff, and what action was taken):	
Review Date:	
Result of Review:	
Signature (Head of School):	Date:
Signature (Governor):	Date:

APPENDIX 2

OVERARCHING RISKS AND DEFINITIONS

Preventing Radicalisation

The Counter-Terrorism and Security Act 2015 places a duty on specified authorities, including local authorities and childcare, education and other children's services providers, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism ("the Prevent duty").

There is a recognition that the world is online and young people can access thousands of websites from their pockets - anywhere. In this way, young people may be exposed to extremist influences or prejudiced views, in particular those via the internet and other social media. An enormous number of extremist websites exist online that are very easily accessible by young people, thus making it possible for children to be treated as prime targets and groomed online. There is also a risk of children being fed propaganda messages via mobile technologies away from the presence of adults.

Example indicators that an individual is engaged with an extremist group, cause or ideology include: spending increasing time in the company of other suspected extremists; changing their style of dress or personal appearance to accord with the group; their day-to-day behaviour becoming increasingly centred around an extremist ideology, group or cause; loss of interest in other friends and activities not associated with the extremist ideology, group or cause; possession of material or symbols associated with an extremist cause (e.g. the swastika for far-right groups); attempts to recruit others to the group/cause/ideology; or communications with others that suggest identification with a group/cause/ideology.

Example indicators that an individual has an intention to use violence or other illegal means include: clearly identifying another group as threatening what they stand for and blaming that group for all social or political ills; using insulting or derogatory names or labels for another group; speaking about the imminence of harm from the other group and the importance of action now; expressing attitudes that justify offending on behalf of the group, cause or ideology; condoning or supporting violence or harm towards others; or plotting or conspiring with others.

Example indicators that an individual is capable of contributing directly or indirectly to an act of terrorism include: having a history of violence; being criminally versatile and using criminal networks to support extremist goals; having occupational skills that can enable acts of terrorism (such as civil engineering, pharmacology or construction); or having technical expertise

that can be deployed (e.g. IT skills, knowledge of chemicals, military training or survival skills).

The examples above are not exhaustive and vulnerability may manifest itself in other ways. There is no single route to terrorism nor is there a simple profile of those who become involved. For this reason, any attempt to derive a 'profile' can be misleading. It must not be assumed that these characteristics and experiences will necessarily lead to individuals becoming terrorists, or that these indicators are the only source of information required to make an appropriate assessment about vulnerability.

Cyberbullying

Cyberbullying is when someone bullies another over the internet or on a mobile 'phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about.

Online Grooming

Pupils may meet people online who aren't who they say they are. This could take place in a game online (Many games now are linked to the internet and players across the globe). Grooming is a word used to describe people befriending children in order to take advantage of them for sexual purposes. Grooming usually takes place over a long period of time. In cases of sexual predators and radicalisation, friendships with unsuspecting children are built up over a time span of 2-3 years.

Sexting

Sexting is when a young person takes an indecent image of them self and sends this to their friends or boy/girlfriends via mobile phones. There are a number of definitions of sexting but, for the purposes of this advice, sexting is simply defined as images or videos generated by children under the age of 18 or of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know. The problem is that, once taken and sent, the sender has lost control of these images and these images could end up anywhere. They could be seen by the child's future employers, their friends or even by child sex offenders.

By having in their possession, or distributing, indecent images of a person under 18 on to someone else – young people are not even aware that they could be breaking the law as these are offences under the Sexual Offences Act 2003. (Child Exploitation and Online Protection (CEOP), 2015).

There are many different types of sexting and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. It is important to apply a consistent approach when dealing with an incident to help protect yourself, the school and the pupil. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff should be familiar with this policy.

APPENDIX 3

Steps to take in the case of an incident of Sexting

STEP 1: Disclosure by a Child

Sexting disclosures should follow the normal safeguarding practices and protocols. A child is likely to be very distressed especially if the image has been circulated widely and, if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to Children's Services.

The following questions will help decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate? Are the school child protection and safeguarding policies and practices being followed? For example, has the Designated Safeguarding Lead (DSL) for child protection advised and support available?
- How widely has the image been shared and is the device in the pupil's possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and or protection?
- Are there other pupils and or young people involved?
- Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, we must ensure school safeguarding and child protection policies and practices are adhered to.

STEP 2: Searching a device

It is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device - it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device. It is important to establish the location of the image but be aware that this may be distressing for the young person involved so be conscious of the support they may need.

The revised Education Act 2011 brought to bear significant new powers and freedoms for teachers and schools. Essentially, the Act gives schools and/or teachers the power to seize and search an electronic device.

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography.

When searching a mobile device, the following conditions should apply:

- The action is in accordance with the school's child protection and safeguarding policies.
- The search is conducted by the Head or a person authorised by them.
- A member of the safeguarding team is present.
- The search is conducted by a member of the same sex.

If any illegal images of a child are found, the school must consider whether to inform the police. If an "experimental" incident is not referred to the police, the reasons for this should be recorded in writing. Always put the child first. Do not search the device if this will cause additional stress to the pupil/person whose image has been distributed. Never search a mobile device (even in response to an allegation or disclosure) if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem. Print out any material for evidence and move any material from one storage device to another.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

Always inform the school's Designated Safeguarding Lead for child protection and record the incident on the 'Online Safety Incident log' sheet and/ or Report a Concern on MyConcern.

If there is an indecent image of a child on a website or a social networking site, we will report the image to the site hosting it. In the case of a sexting incident involving a child or young person where we feel that they may be at risk of abuse, we will report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

STEP 3 - What to do and not do with the image.

If the image has been shared across a personal mobile device:

- Always confiscate and secure the device(s).
- Never view the image unless there is a clear reason to do so or send, share or save the image anywhere.

If the image has been shared across a school network, a website or a social network:

- Always block the network to all users and isolate the image.

STEP 4 - Who should deal with the incident?

Ensure the Designated Safeguarding Lead (DSL) and Head of School are involved in dealing with the incident.

The DLP should always record the incident. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first.

STEP 5 - Deciding on a response

There may be a multitude of reasons why a student has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere. We will make a referral to LADO, if needed and contact the police (if appropriate).

Online reputation

The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It's important that children and adults understand how to manage their online reputation and the impacts for them of a negative online reputation.