Online Safety Policy

Date Drafted: October 2009
Last Revision: 18th November 2019
Review Date: November 2022
Authors: Sue Burke/Toni Edmonds-Smith

Agreed by Safeguarding and Premises Committee

Signed: Dated:
(Chair of Committee)

'Every Achievement Counts'

Online Safety at Greenmead School

Context

Greenmead is a primary school for pupils with learning difficulties, additional physical disabilities, significant communication difficulties and many have additional complex medical conditions.

Online safety encompasses internet technologies and electronic communications such as mobile phones. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Most pupils at Greenmead are unable to access the internet without full adult support and those who are, are closely supervised.

Aims

This policy aims to ensure:

- Responsible ICT used by all staff and pupils.
- Sound implementation of online safety in both administration and the curriculum, including secure network design and use.
- Safe and secure internet connections and filtering systems.

Teaching and Learning

The internet is an essential element in everyday life for education, business and social interaction. The school has a duty to provide relevant and curriculum enhancing internet access to pupils as deemed appropriate to their learning needs.

At Greenmead, the pupils will be able to access the internet with appropriate support. This may be in the form of browsing websites with appropriate internet filtering in place and adult guidance or inserting pictures and videos taken from internet sources into switch accessible programmes or in printed format where more appropriate.

Where relevant, pupils will be taught what internet use is acceptable and what is not and will be given clear lesson objectives for internet use, planned for in half termly ICT planning. We will ensure that the use of internet derived materials by staff and pupils, complies with the copyright law.

Any pupils at Greenmead, who are using email as part of their curriculum for ICT, will be given a school approved email address. Their use will be carefully monitored and emails will be shared within lessons. This ensures that any offensive material will be screened and removed and pupil's personal details will not be disclosed.

School Website

- Personal information i.e. photographs, will only appear on the website for the legitimate needs of the school.
- Written permission from parents or carers will be obtained before carefully selected photographs are published on the school website.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Filtering

- Pupils' access to social networking sites will be blocked but access for specific supervised activities may be allowed.
- News groups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- The school will work with the LA and IT Support to ensure that systems to protect the pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to a Safeguarding Lead.

Video-Conferencing

- Any video-conferencing activities will be carefully planned for and will use the internet, using a web filter to enable and disable access as required.
- Pupils will only access video-conferencing with staff permission and supervision.

Systems Management

- ICT systems will be reviewed regularly by the IT Manager and the Deputy Head.
- Virus protection will be updated regularly and filtering systems will be in place.

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.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations and Data Protection Act 2018.

Authorising Internet Access

- All staff must read and sign the 'Data Protection and Online Safety' contract (See Appendix 1) before using any ICT resource.
- The school enables all staff and pupils to have internet access, protected by web filter.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale of the internet, it is not possible to guarantee that unsuitable material will never appear on a computer. Neither the school nor Wandsworth Council can accept liability for the material access or any consequences of internet access. No pupils will be allowed unsupervised access to the internet at Greenmead.
- The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to a member of the senior leadership team.

Links to other policies

This policy should be read in conjunction with the ICT curriculum policy and the Safeguarding Policy.

Please also see the Data Protection and Online Safety Contract (Appendix 1).

Dissemination and review

This policy will be disseminated widely.

- Discussed in whole school meeting
- Data Protection and Online Safety contract will be given and signed for by new employees at induction

Appendix 1

Data Protection and Online Safety

Data Protection- personal data

Personal data refers to an individual's information i.e. (1) Name, (2) Address and telephone number and (3) Date of Birth. When using any personal data the user must ensure that this is not shared unwillingly.

To reduce the risk of personal data being unwilling shared or taken; all Greenmead staff and volunteers must

- Never use all three elements of personal data unless completely necessary. If you feel it is completely necessary ensure any documents containing this information that leave the Greenmead site are securely locked away when not in use.
- When working at home on documents which contain personal data, photos or video use an encrypted memory stick. These sticks will be assigned to you by the IT Manager. You must not lend this stick to anyone else. You must return the stick to School Business Manager or IT Manager on request. If you lose the stick you must inform either of these people straight away. Any lost sticks will be reported to the Data Protection Officer. You must assign a password to Microsoft documents to prevent unwanted viewing or editing of the document. Notify the recipient of the password in a separate email. (If you do not know how to set a password see the IT Manager)
- You must not download any documents from your encrypted memory stick onto your personal computer.
- If attending meetings which require you to take hard copies with personal data with you, inform Head or Deputy. To reduce personal data being taken out of the school it is recommended that you email the information to yourself rather than carry hard copies. If you are given hard copies at a meeting ask the chair to email the details and leave hard copy at meeting.
- Ensure smart phones and iPads have code activated log in.
- If you have personal data at home e.g. phone numbers for school closure, it is your responsibility to keep them in a safe place, away from visitor's view.
- When you resign and leave the school you will be required to return this information to the school so that you do not have access to information about the school. You will also be required to return the encrypted memory stick.
- When emailing never put personal data in the subject box. The main body of text should only have essential personal data. Emailing within the school network holds less risk than emailing outside our network. If the email contains sensitive information use Egress email only. If you do not have an Egress account please see a member of Senior Leadership Team (SLT).
- All emails must be sent via school email, your personal email should not be used for work related matters.
- Only use your school email account for school business i.e. do not use the school email for personal reasons or use if for online services for non-school activities.
- Do not store personal data on your personal computers, laptops, hard drives or memory sticks.
- Do not print out any personal data at home or off site.
- If using the school mobile phone this must be assigned to you and you will be responsible for its security.
- Any lost or stolen devices or phones should be reported as a Data Breach immediately to a member of SLT. This will then be reported to the Data Protection Officer.

Pictures and videos

- Do not use your own camera or phone to take photos/videos of the pupils
- When storing photos do not use personal data to name files
- Do not allow volunteers or parents to take photos or videos of the pupils unless you are sure all pupils have given permission. If you are allowing others to use a camera/phone/video you must inform them that they may only use this data for personal use; they are not permitted to place on social networking sites.
- If editing videos of pupils at home an encrypted memory stick, do not store on hard drive.

Social Networking Sites

Due to the public nature of social networking sites we recommend staff and volunteers to be extremely cautious in their use. We advise staff members are not "friends" with parents/carers as this can cause unnecessary difficulties when least expected. If however you are already "friends" or family members we suggest the following

- Do not become friends with any new parents- politely inform them that it is school policy to ensure equality for all the pupils
- Never comment on school related issues
- If you witness any breech of this code of conduct you should report it to a member of SLT.

I fully understand and agree to all terms of this contract

Signed..... Name..... Date.....