RED HOUSE SCHOOL

GENERAL DATA PROTECTION REGULATIONS (GDPR)

This policy relates to all sections and activities of the school and its pupils, e.g. the Senior School, the Junior School (including EYFS), Wrap Around Care, Offsite Activities and school run Holiday Activities or Clubs. The policy also applies to incidents involving our pupils out of school hours.

1 AIMS OF THIS POLICY

1.1 The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data.
- How personal data should be processed, stored, archived and disposed of.
- How staff, parents and pupils can access personal data.

2 GDPR PRIVACY NOTICE

2.1 The Head has ultimate responsibility for the implementation and management of this Privacy Notice and will support the Head of Finance and Compliance and the Head of Marketing in this respect.

2.2 This Privacy Notice is intended to provide information about how the school will process personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to as parents).

2.3 Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware to comply with this Privacy Notice which also provides further information about how personal data about those individuals will be used.

2.4 This Privacy Notice also applies to the School's other relevant terms and conditions and policies covering:

- Any contract between the school and its staff or the parents of pupils.
- Taking, storing and using images of children including CCTV.
- Retention of records.
- Safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded.
- The use of ICT.

3 RESPONSIBILITY FOR DATA PROTECTION

3.1 The Board of Governors and the Head are responsibility for Data Protection, and will appoint a Data Protection Officer to manage data.

3.2 The School has appointed the Head of Finance and Compliance as the Data Protection Officer (DPO), who will deal with all your requests and enquiries concerning the School's use of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection law.

3.3 The role of the DPO will include:

- To inform and advise the organisation and its employees about their obligation to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

3.4 Everyone in the school has the responsibility of handling personal information in a safe and secure manner. Data will be processed and handled by all members of staff but only within the context of their role.

3.5 Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (employees, pupils, parents, etc.).

3.6 The Head of Finance and Compliance can be contacted at the School via telephone 01642 553370.

4 WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

4.1 In order to carry out its ordinary duties to staff, pupils and parents, the School needs to process a wide range of personal data about individuals as part of its daily operation.

4.2 Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

4.3 Other uses of personal data will be made in accordance with the School's legitimate interests.

4.4 The School expects that the following uses will fall within that category of its (or its communities) legitimate interests:

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents).
- To provide education services, including musical education, physical training or spiritual development, career services, and co-curricular activities to pupils, and monitoring pupils' progress and educational needs.
- Maintaining relationships with alumni and the school community, including direct marketing or fundraising activity.
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law, such as, tax, diversity or gender pay gap analysis.
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents, as appropriate.
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils.
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school.
- To safeguard pupils' welfare and provide appropriate pastoral care.
- To monitor, as appropriate, use of the School's ICT and communications systems, in accordance with the School's ICT policies.
- To make use of photographic images of pupils in School publications, on the School website and on the School's social media channels in accordance with the School's policies covering the use of CCTV and taking, storing and using images of children.
- To carry out or cooperate with any school or external complaints, disciplinary or investigation process.
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

4.5 In addition, the School will on occasion need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

- To safeguard pupils' welfare and provide appropriate pastoral and/or medical care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of school trips who need to be made aware of dietary or medical needs.
- To provide educational services in the context of any special educational needs of a pupil.
- In connection with employment of its staff, for example DBS checks, welfare, union membership or pension plans.
- As part of any school or external complaints, disciplinary or investigation process that involves such data, for example, if there are SEND, health or safeguarding elements.
- For legal and regulatory purposes; for example, child protection, diversity monitoring and health and safety, and to comply with its legal obligations and duties of care.

5 TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

5.1 Personal Data

5.1.1 The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records.

5.1.2 Personal data will include:

- Personal information about members of the school community – including pupils, members of staff and parents e.g. names, addresses, contact details (email and telephone), legal guardianship contact details, disciplinary records, etc.
- Curricular/academic data e.g. class lists, pupil progress records, reports, references, etc.

- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references.
- Car details about those who use our car parking facilities.
- Bank details and other financial information, e.g. about parents who pay fees to the School.
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any SEND), and examination scripts and marks.
- Personnel files, including in connection with academics, employment or safeguarding.
- Where appropriate, information about individuals' health and welfare, and contact details for their next of kin.
- References given or received by the School about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils.
- Correspondence with and concerning staff, pupils and parents past and present.
- Images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the School's CCTV system (in accordance with the School's policy and procedures on taking, storing and using images of children).
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

5.2 Special Category Data

5.2.1 'Special Category Data' is more sensitive, and so needs more protection. In a school the most likely special category data is likely to be:

- Information on the racial or ethnic origin of a pupil or member of staff.
- Information about the sexuality of a child, his or her family or a member of staff.
- Medical or SEND information about a child or member of staff.
- Some information regarding safeguarding will also fall into this category.

5.3 Other types of Data not covered by the Act

5.3.1 This is data that does not identify a living individual and could include lesson plans (where no individual pupil is named), teaching resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance, the school calendar for the forthcoming year).

6 HOW THE SCHOOL COLLECTS DATA

6.1 Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents).

6.2 This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments). However, in some cases personal data will be supplied by third parties; e.g. another school, or other professionals or authorities working with that individual.

7 WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

7.1 Occasionally, the School will need to share personal information with third parties who have equalled the School's precautions, systems and procedures for dealing with data in line with current data protection legislation.

7.2 Information will be shared with third parties such as:

- Professional advisers (e.g. lawyers, insurers, accountants).
- Government authorities (e.g. HMRC, Department for Education (DfE), police or the local authority).
- Appropriate regulatory bodies (e.g. Charities Commission, Companies House).
- ICT software providers; caterers; photographers; PR agencies.

7.3 For the most part, personal data collected by the School will remain within the school, and will be processed by appropriate individuals in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of medical records held and accessed only by the appropriate staff.

7.4 However, a certain amount of any SEND pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

7.5 Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including, Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities, such as, the Children's HUB, the LADO or the police. For further information about this, please view the School's Child Protection (Safeguarding) Policy.

7.6 Finally, in accordance with Data Protection law, some of the School's processing activity is carried out on its behalf by third parties, such as ICT systems, web developers or cloud storage providers. This is always

subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

8 HOW LONG WE KEEP PERSONAL DATA

8.1 The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. If you have any specific queries about how our retention policy is applied, or wish to request that personal data you no longer believe to be relevant is considered for erasure, please contact the Head of Finance and Compliance at the School. However, please bear in mind that the School will often have lawful and necessary reasons to hold on to some personal data even following such request.

8.2 A limited and reasonable amount of information will be kept for archiving purposes, for example and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a 'suppression record').

9 KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

9.1 The School will use the contact details of parents to keep them updated about the activities of the school, alumni and parent events of interest; including; by sending updates and newsletters, by email and by post.

9.2 Unless the relevant individual objects, the School will also:

- Share personal data about parents, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Parent Teachers Association (PTA) and Alumni.
- Contact parents by post and email in order to promote and raise funds for the school and, where appropriate, other worthy causes.
- Should you wish to limit or object to any such use, or would like further information about them, please contact the Head of Marketing, in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the school is likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

10 YOUR RIGHTS

10.1 Rights of access

10.1.1 Individuals have various rights under Data Protection law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or have it transferred to others, or for the school to stop processing it – but subject to certain exemptions and limitations. Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Head of Finance and Compliance.

10.1.2 The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information.

10.1.3 The School will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, the school may ask you to reconsider, or require a proportionate fee (but only where Data Protection law allows it).

10.2 Requests that cannot be fulfilled

10.2.1 You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example, legal advice given to or sought by the School, or documents prepared in connection with a legal action).

10.2.2 The School is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by the School itself for the purposes of the education, training or employment of any individual.

10.2.3 You may have heard of the 'right to be forgotten'. However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your, or your child's, personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this Privacy Notice. All such requests will be considered on their own merits.

10.3 Pupil requests

10.3.1 Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making (see section 'Whose rights?' below). A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

10.3.2 Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's: for older pupils, the parent making the request may need to evidence their child's authority for the specific request.

10.3.3 Pupils aged 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home.

10.4 Parental requests

10.4.1 It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The School may consider there are lawful grounds for sharing with or without reference to that pupil.

10.4.2 Parents will in general receive educational and pastoral updates about their children, in accordance with the Parent Contract. Where parents are separated, the School will, in most cases, aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child.

10.4.3 All information requests from, on behalf of, or concerning pupils, whether made under subject access or simply as an incidental request, will therefore be considered on a case by case basis.

10.5 Consent

10.5.1 Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time, subject to similar age considerations, as above. Examples where we do rely on consent are biometrics, certain types of uses of images, certain types of fundraising activity. Please be aware however that the school may not be relying on consent but have another lawful reason to process the personal data in question even without your consent.

10.5.2 That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual; e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested.

10.6 Whose rights?

10.6.1 The rights under Data Protection law belong to the individual to whom the data relates. However, the School will often rely on parental authority or notice for the necessary ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the school relying on strict consent. Please refer to the section on 'Consent' above.

10.6.2 Where consent is required, it may in some cases be necessary or appropriate, given the nature of the processing in question, and the pupil's age and understanding, to seek the pupil's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

10.6.3 In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare. That is unless, in the School's opinion, there is a good reason to do otherwise.

10.6.4 However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; e.g. where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

10.6.5 Pupils are required to respect the personal data and privacy of others, and to comply with the School's policies and rules. Staff are under professional duties to do the same, covered under the relevant staff policies.

11 DATA ACCURACY AND SECURITY

11.1 The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible.

11.2 Individuals must notify the person named below of any significant changes to important information, such as contact details, held about them.

- Prospective parents — Head of Admissions
- Current parents — School Secretaries

- Employees — Head of Finance and Compliance
- Alumni — Head of Marketing
- Governors — Head of Admissions

11.3 An individual has the right to request any out-of-date, irrelevant or inaccurate or information about them is erased or corrected, subject to certain exemptions and limitations under Data Protection law. Please see above for details of why the school may need to process your data, of who you may contact if you disagree.

11.4 The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under Data Protection law and receive relevant training.

12 BREACHES OF DATA PROTECTION

12.1 The Information Commissioner's Office (ICO) website defines a breach of data as:

'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.'

12.2 Where a potential breach of data has been identified, the school will refer to current ICO guidelines in order to effectively and lawfully deal with the incident(s). A link to the website outlining how to deal with a potential breach of data is shown here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

13 RESPONDING TO A CYBER ATTACK

13.1 Please refer to Section 8 of the School's Disaster Response Policy or Appendix 3 for further details.

14 PRIVACY NOTICE

14.1 The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

15 QUERIES AND COMPLAINTS

15.1 Any comments or queries on this policy should be directed to the Head of Finance and Compliance and using the School's contact details.

15.2 If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection law, they should utilise the school complaints/grievance procedure and should also notify the Head of Finance and Compliance.

15.3 They can also make a referral to or lodge a complaint with the ICO, although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

Reviewed by: Dr R Ashcroft and Mr C Staniford
February 2024

Ratified by: The Health and Safety Committee of the Board of Governors
February 2024

APPENDIX 1 – LINKS TO RESOURCES AND GUIDANCE

ICO Guidance on GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Specific information for schools is available here. This includes links to guides form the DfE:
http://ico.org.uk/for_organisations/sector_guides/education

Specific information about CCTV:
http://ico.org.uk/for_organisations/data_protections/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit:
A downloadable scheduled for all records management in schools
http://irms.org.uk/page/SchoolsToolkit

Disclosure and Barring Service (DBS)
Details of storage and access to DBS certificate information:
https://www.gov.uk/government/publications/handling-of-dbs-certificateinformation/handling-of-dbs-certificate-information

DfE Privacy Notices
https://www.gov.uk/government/pulications/data-protection-and-privacy-privacy-notices

DfE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biomentric-information-ofchildren-in-schools

APPENDIX 2 - PRIVACY AND COOKIES

1 PRIVACY POLICY

1.1 This privacy policy sets out how Red House School uses and protects any information that you give us when you use this website.

1.2 Red House School is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

1.3 Red House School may change this policy from time to time by updating this policy. You should check this policy from time to time to ensure that you are happy with any changes.

2 WHAT WE COLLECT

2.1 We may collect the following information:

- Name.
- Contact information including email address.
- Demographic information, such as postcode, preferences and interests.
- Photograph (if uploaded).
- Other information relevant to customer surveys and/or offers.

3 WHAT WE DO WITH THE INFORMATION WE GATHER

3.1 The data that you give to us is used by the School to provide you with relevant documentation, such as the School Prospectus or recruitment information.

3.2 We do not use the information you provide us with for marketing or publicity purposes.

4 SECURITY

4.1 We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. N.B. Data transmission over the internet is inherently insecure and we cannot guarantee the security of data sent over the internet.

5 LINKS TO OTHER WEBSITES

5.1 Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website.

5.2 Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement.

5.3 You should exercise caution and look at the privacy statement applicable to the website in question.

6 COOKIES

6.1 What are cookies and how are they used?

6.1.1 A cookie is a small file, typically of letters and numbers, downloaded on to a device when the user accesses certain websites.

6.1.2 Cookies are then sent back to originating website on each subsequent visit. Cookies are useful because they allow a website to recognise a user's device. They are used to remember useful information that allows certain functionality to work.

6.1.3 Cookies cannot harm your computer, and are active for differing lengths of time, some are stored until you close your browser, while others may last for several weeks or more.

6.2 How we use cookies?

6.2.1 The Red House School website has a variety of useful features and tools, and to make best use of them your computer, tablet or mobile device will need to accept cookies. We can only provide you with certain features by using cookies. If you have chosen to disable cookies you will still be able to browse the website, but some functions may be unavailable.

6.2.2 We also use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We use this information for statistical analysis purposes and then the data is removed from the system.

6.2.3 Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

6.2.4 You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

6.3 How do I change my cookie settings?

6.3.1 By default, cookies should be enabled on your computer or device. If not, your experience on many websites will be limited.

6.3.2 If you would prefer to restrict, block or delete cookies from Red House School or any other website, you can use your internet browser to do this. Each browser is different, so check the 'help' menu on your browser to learn how to change your cookies preferences, or visit www.allaboutcookies.org/manage-cookies

APPENDIX 3 – RESPONDING TO A CYBER ATTACK

1.1 According to the Department of Education's 'Meeting Digital and Technology Standards in Schools and Colleges' (March and October 2022) 'being unprepared for a cyber-attack can lead to poor decisions, slow recovery and expensive mistakes. A good response plan made ahead of time will speed up your response, reduce stress levels and confusion. Effective response will reduce the material, reputational and safeguarding damage from ransomware attacks.'

1.2 Cyber-attacks are crimes against a school that need to be investigated so perpetrators can be found and counter-measures identified. A cyber-attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or system. An attack could be made by a person outside or inside the school.

1.3 This compromise of data might include:

- Stealing the data.
- Copying the data.
- Tampering with the data.
- Damaging or disrupting the data, or similar.
- Unauthorised access.

1.4 The School's IT service provider and Network Manager will notify the School's Senior Management Team (SMT) of all cyber-attacks. Appropriate action and information-sharing must be carried out in accordance with the General Data Protection Regulation (GDPR).

1.5 The Head will report the incident to the Board of Governors via the Chair of Governors.

1.6 Where a data breach has or may have occurred, the Head of Finance and Compliance or the Head will report to the Information Commissioner's Office (ICO). These incidents will also be reported to the Department of Education's Sector Cyber Team at Sector.Incidentreporting@education.gov.uk

1.7 The Head of Finance and Compliance or the Head will report any suspicious cyber incident to Action Fraud on 0300 123 2040 or on the Action Fraud website.

1.8 The Head of Finance and Compliance or the Head will also report any incidents to the police. The police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

1.9 The Head and Head of Finance and Compliance will exercise judgement in reporting. Incidents where any compromise may have taken place or other damage was caused should be reported. But receipt of a phishing email alone, for example, does not require reporting to the Department of Education but can be reported to Action Fraud at report@phishing.gov.uk.

1.10 Where the incident causes long term school closure or serious financial damage, the Head will also inform the National Cyber Security Centre.

1.11 To mitigate against a cyber-attack in school, all staff with access to the school ICT networks to be trained annually in the basics of cyber security, as having this knowledge amongst staff and governors is vital in promoting a more risk aware school culture. The Governor with Health & Safety responsibility also completes the training. The training accessed by staff and the governor is the following NCSC course - https://www.ncsc.gov.uk/information/cyber-security-training-schools

1.12 This NCSC training on 'Cyber Security in Schools' focuses on:

- Phishing.
- Password security.
- Social engineering.
- The dangers of removable storage media.